ATLANTIS AND
where solutions begin

I-Fly Wireless Router ADSL

4 Fast Ethernet ports, Firewall, VPN with 3DES accelerator

A02-WRA4-54G

User's Reference Guide
V1.0

FAST SWAP
3 YEARS WARRANTY

HELP DESK
SERVICE

Company certified ISO 9001:2000

Copyright

The Atlantis Land logo is a registered trademark of Atlantis Land SpA. All other names mentioned mat be trademarks or registered trademarks of their respective owners. Subject to change without notice. No liability for technical errors and/or omissions.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Important Note

The antenna(s) used for this equipment must be installed to provide a separation distance of at least 30 cm from all persons.

This equipment must not be operated in conjunction with any other

Table of Contents

CHAPTER 1 1

1.1 AN OVERVIEW OF THE ADSL FIREWALL ROUTER 1

1.2 PACKAGE CONTENTS 2

1.3 I-FLY WIRELESS ROUTER ADSL FEATURES 2

1.4 I-FLY WIRELESS ROUTER ADSL APPLICATION 5

CHAPTER 2 6

2.1 CAUTIONS FOR USING THE I-FLY WIRELESS ROUTER ADSL 6

2.2 THE FRONT LEDS 6

2.3 THE REAR PORTS 7

2.4 CABLING 7

CHAPTER 3 8

3.1 BEFORE CONFIGURATION 8

3.2 CONNECTING THE I-FLY WIRELESS ROUTER ADSL 8

3.3 CONFIGURING PC IN WINDOWS 9

For Windows 95/98/ME 9

For Windows NT4.0 11

For Windows 2000 12

For Windows XP 14

3.4 FACTORY DEFAULT SETTINGS 16

3.4.1 Username and Password 16

3.4.2 LAN and WAN Port Addresses 16

3.5 INFORMATION FROM THE ISP 17

3.6 CONFIGURING WITH THE WEB BROWSER 17

3.6.1 STATUS 18

3.6.2 Quick Start 20

3.6.3 Configuration 20

3.6.3.1 LAN 20
3.6.3.1.1 Ethernet 21
3.6.3.1.2 Wireless 21
3.8.2.1.3 Wireless Security 22
3.6.3.1.4 Port Settings 23
3.6.3.1.5 DHCP 24
3.6.3.2 WAN 25
3.6.3.2.1 ISP 25
3.6.3.2.2 DNS 30
3.6.3.2.3 ADSL 30
3.6.3.3 System 30
3.6.3.3.1 Time Zone 31
3.6.3.3.2 Remote Access 31
3.6.3.3.3 Firmware Upgrade 32
3.6.3.3.4 Backup / Restore 32
3.6.3.4 Firewall 33
3.6.3.4.1 Configuring Packet Filter 35
3.6.3.4.2 INTRUSION DETECTION 37
3.6.3.4.3 MAC Filtering 39
3.6.3.4.4 URL Filtering 39
3.6.3.4.5 Firewall Log 41
3.6.3.5 VPN 42
3.6.3.6 QoS 57
3.6.3.6.1 Prioritization 57
3.6.3.6.2 IP Throttling 58
3.6.3.7 Virtual Server 59
3.6.3.8 Advanced 60
3.6.3.8.1 Static Routing 60
3.6.3.8.2 Dynamic DNS 61
3.6.3.8.3 Check EMails 61
3.6.8.3.4 Device Management 62
3.6.4 Save Configuration to Flash 65
3.6.5 Logout 65

CHAPTER 4 66
PROBLEMS STARTING UP THE ADSL FIREWALL ROUTER 66
PROBLEMS WITH THE WAN INTERFACE 66
PROBLEMS WITH THE LAN INTERFACE 66

APPENDIX A 67
TECHNICAL FEATURES 67

APPENDIX B..... 68
SUPPORT..... 68

Chapter 1
Introduction

1.1 An Overview of the ADSL Firewall Router

Broadband Sharing and IP sharing
The I-Fly Wireless Router ADSL supports 4 ports 10/100 Mbps auto-negotiating Fast Ethernet for connection to your local area network (LAN) and downstream (with built-in ADSL modem) rate up to 8Mbps.
With integrated IEEE802.11g Wireless Access Point, the device offers quick and easy access among wired network and wireless network. The I-Fly Wireless Router also supports WPA security, it increases the level of data protection and access control for Wireless LAN.
Power by NAT technology, dozens of network users can surf on the Internet and share the ADSL connection simultaneously by using one ISP account and one single IP address. Firmware upgradeable to ADSL2.

Quality of Service and IP Throttling
QoS gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring important data like gaming packets move through the router at lightning speed, even under heavy load.
If you have ever found your net speed has slowed to a crawl because another family member is using a P2P file sharing program, you'll understand why the Quality of Service (QoS) features on the router are such a breakthrough.
Using IP Throttling, bandwidth limits can be enforced on any system within your LAN, or even on a particular application.

Firewall Security with (SPI, DoS) and VPN (IPSec, PPTP)
The I-Fly Wireless Router ADSL offers not only NAT but also provides powerful firewall, which are able to filter the advanced hacker pattern. It can automatically detect and block Denial of Service (DoS) attacks and thanks to the ability of Stateful Packet Inspection (SPI) it determines if a data packet is allowed through the firewall to the private Lan. It manages the VPNs IPSec or PPTP, for establishing a private tunnel over the public Internet to ensure transmission security between two or more sites. With built-in DES/3DES accelerator, the router enhances the IPSec VPN performance significantly. Up to 16 simultaneous VPN tunnels are supported.

Easy Configuration and Management
Support web based GUI, Telnet and Hyperterminal for configuration and management. Also supports remote management (Web and telnet) capability for remote user to configure and manage this product. It incorporates besides a client DynamicDNS

1.2 Package Contents

- One I-Fly Wireless Router ADSL
- One CD-ROM containing the online manual
- One Quick Start Guide
- One RJ-11 ADSL/telephone cable
- One CAT-5 LAN cable
- One AC-DC power adapter (12VDC, 1A)
- One PS2-RS232(DB9) cable

If any of the above items are missing, please contact your reseller.

1.3 I-Fly Wireless Router ADSL Features

Wireless ADSL Firewall Router provides the following features:

- **ADSL Multi-Mode Standard:** Supports downstream transmission rates of up to 8Mbps and upstream transmission rates of up to 1024Kbps. It also supports rate management that allows ADSL subscribers to select an Internet access speed suiting their needs and budgets. It is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G992.2).

- **Upgradeable to ADSL2:** Supports downstream transmission rates of up to 12Mbps

- **Wireless Ethernet 802.11g:** With built-in 802.11g access point for extending the communication media to WLAN while providing the WEP and WPA for securing your wireless networks. The I-Fly Wireless Router ADSL has included the first solution for turbo charging 802.11g systems called PRISM Nitro. It provides up to 50% greater throughput performance in homogenous 802.11g networks and enhanced protection mechanisms to significantly increase mixed-mode network performance.

- **Fast Ethernet Switch:** A 4-port 10/100Mbps fast Ethernet switch is supported in the LAN site and automatic switching between MDI and MDI-X for 10Base-T and 100Base-TX ports is supported. An Ethernet straight or cross-over cable can be used directly, this fast Ethernet switch will detect it automatically.

- **Quality of Service and IP Throttling :** QoS gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring important data like gaming packets move through the router at lightning speed, even under heavy load. If you have ever found your net speed has slowed to a crawl because another family member is using a P2P file sharing program, you'll understand why the Quality of Service (QoS) features on the router are such a breakthrough. Using IP Throttling, bandwidth limits can be enforced on any system within your LAN, or even on a particular application.

- **Multi-Protocol to Establish A Connection:** Supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1577) to establish a connection with the ISP. The product also supports VC-based and LLC-based multiplexing.

- **Quick Installation Wizard:** Supports a WEB GUI page to install this device quickly. With this wizard, an end user can enter the information easily which they from the ISP, then surf the Internet immediately.

- **Universal Plug and Play (UPnP) and UPnP NAT Traversal:** This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors. It makes network simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices.

- **Network Address Translation (NAT):** Allows multi-users to access outside resource such as Internet simultaneously with one IP address/one Internet access account. Besides, many application layer gateway (ALG) are supported such as web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting and others.

- **Firewall:** Supports SOHO firewall with NAT technology. Automatically detects and blocks the Denial of Service (DoS) attack. The URL-blocking, packet filtering and SPI are also supported. The hacker's attack will be recorded associated with timestamp in the security logging area. More firewall features will be added continually, please visit our web site to download latest firmware.

- **Domain Name System (DNS) relay:** provides an easy way to map the domain name (a friendly name for users such as www.yahoo.com) and IP address. When a local machine sets its DNS server with this router's IP address, then every DNS conversion requests packet from the PC to this router will be forwarded to the real DNS in the outside network. After the router gets the reply, then forwards it back to the PC.

- **Dynamic Domain Name System (DDNS):** The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. For example, to use the service, you must first apply an account from this free Web server http://www.dyndns.org/. There are more than 5 DDNS servers supported.

- **Virtual Private Network (VPN):** Allows a user to make a tunnel with a remote site directly to secure the data transmission among the connection. Users can use **embedded PPTP client/server** supported by this router to make a VPN tunnel or the user can run the PPTP client in PC and the router already provides IPSec and PPTP pass through function to establish a VPN connection if the user likes to run the PPTP client in his local computer.

- **PPP over Ethernet (PPPoE):** Provide embedded PPPoE client function to establish a connection. Users can get greater access speed without changing the operation concept, sharing the same ISP account and paying for one access account. No PPPoE client software is required for the local computer. The Always ON, Dial On Demand and auto disconnection (Idle Timer) functions are provided too.

- **Virtual Server:** Users can specify some services to be visible from outside users. The router can detect incoming service request and forward it to the specific local computer to handle it. For example, users can assign a PC in a LAN acting as a WEB server inside and expose it to the outside network. Outside users can browse an inside web server directly while it is protected by NAT. A **DMZ** host setting is also provided to a local computer exposed to the outside network, Internet

- **Rich Packet Filtering:** Not only filters the packet based on IP address, but also based on Port numbers. It also provides a higher-level security control.

- **Dynamic Host Control Protocol (DHCP) client and server:** In the WAN site, the DHCP client can get an IP address from the Internet Server Provider (ISP) automatically. In the LAN

site, the DHCP server can allocate up to 253 client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.

- **Static and RIP1/2 Routing:** Supports an easy static table or RIP1/2 routing protocol to support routing capability.

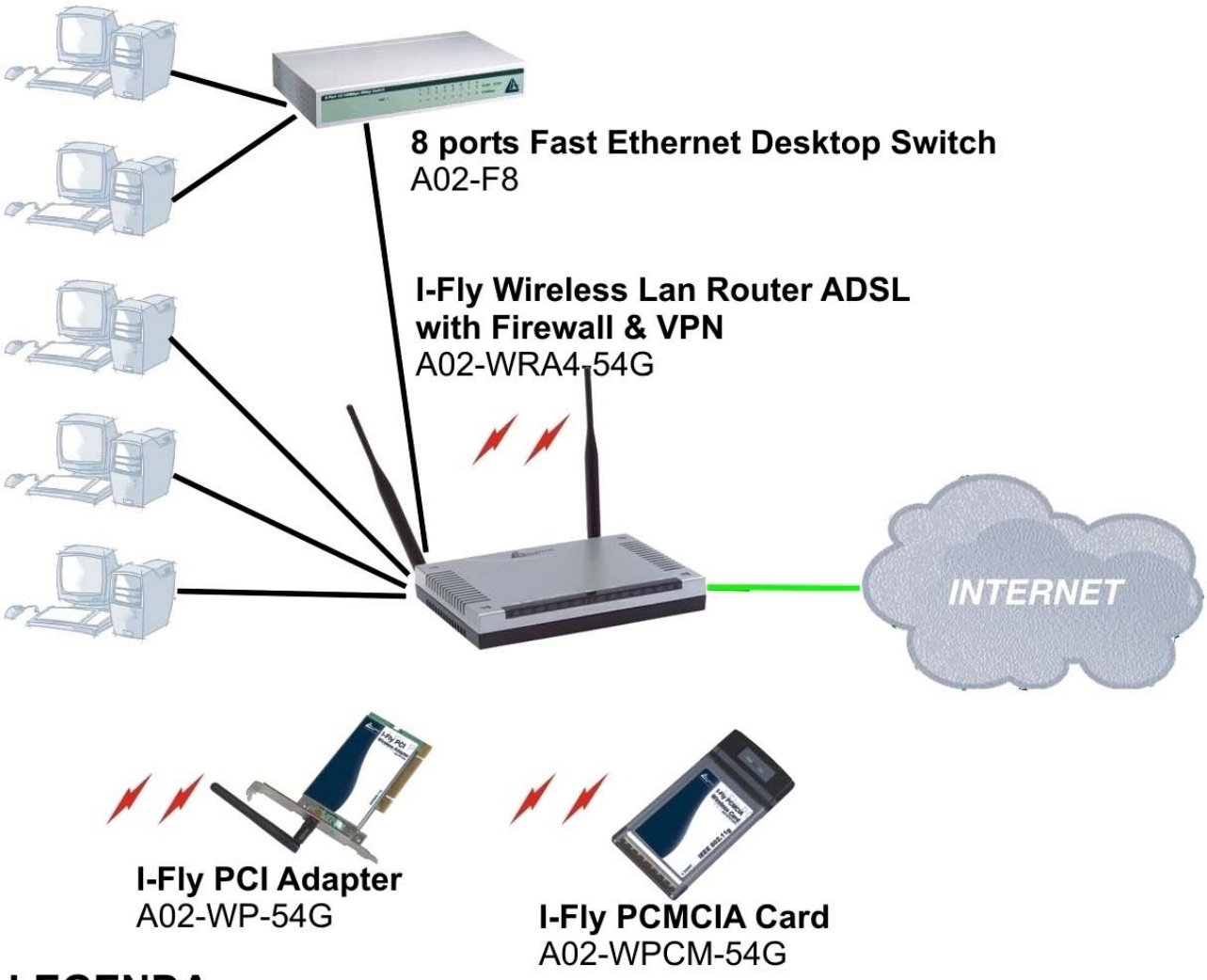
- **SNTP:** An easy way to get the network real time information from an SNTP server.

- **Web based GUI:** supports web based GUI for configuration and management. It is user-friendly with an on-line help, providing necessary information and assist user timing. It also supports remote management capability for remote users to configure and manage this product.

- **Firmware Upgradeable:** the device can be upgraded to the latest firmware through the WEB based GUI.

- **Rich management interfaces:** Supports flexible management interfaces with local console port, LAN port, and WAN port. Users can use terminal application through console port to configure and manage the device, or Telnet, WEB GUI, and SNMP through LAN or WAN ports to configure and manage a device.

1.4 I-Fly Wireless Router ADSL Application



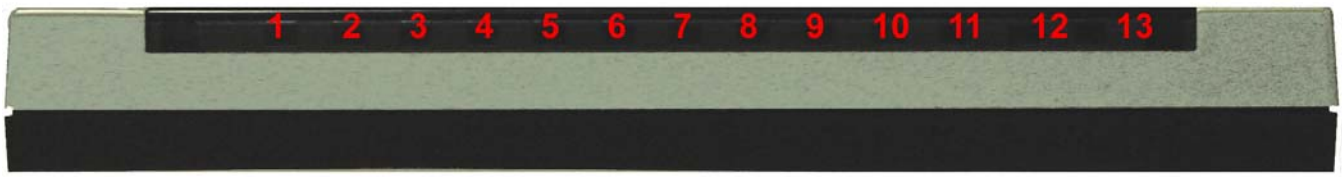
LEGENDA

Chapter 2
Using Wireless ADSL Router

2.1 Cautions for using the I-Fly Wireless Router ADSL

Do not place the ADSL Wireless Router under high humidity and high temperature.
Do not use the same power source for ADSL Wireless Router with other equipment.
Do not open or repair the case yourself. If the ADSL Wireless Router is too hot, turn off the power immediately and have a qualified serviceman repair it.
Place the ADSL Wireless Router on a stable surface.
Only use the power adapter that comes with the package.
Do NOT upgrade firmware on any Atlantis Land product over a wireless connection. Failure of the device may result. Use only hard-wired network connections.

2.2 The Front LEDs



LED		Meaning
1	**Power**	Lit when power ON
2	**Sys**	Lit when system is ready
3-6	**Lan**	Lit when connected to Ethernet device Green for 100Mbps; Orange for 10Mbps Blinking when data transmit/received
7	**WLan**	Lit green when the wireless connection is established. Flashes when sending/receiving data.
10	**Mail**	Blinking when there is email in the email account
11	**PPP**	Lit when there is a PPPoA/PPPoE connection
13	**ADSL**	Lit when successfully connected to an ADSL DSLAM

2.3 The Rear Ports

PORT		MEANING
1	**LINE**	Connect the supplied RJ-11 cable to this port when connecting to the ADSL/telephone network.
2	**PS2(Console)**	Connect a RS-232 cable to this port when connecting to a PC's RS-232 port (9-pin serial port).
3	**LAN 4X (RJ-45 connector)**	Connect an UTP Ethernet cable to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
4	**Reset**	After the device has turned on, press it to reset the device or restore to factory default settings. The operation is as below: **0-3** seconds: reset the device **3-6** seconds: no action **6 seconds or above**: restore to factory default settings (this is used when you can not login to the router, e.g. forgot the password)
5	**PWR**	Connect the supplied power adapter to this jack.
6	**Power Switch**	A Power ON/OFF switch

2.4 Cabling

The most common problem is bad cabling or ADSL line. Make sure that all connected devices are turned on. On the front of the product is a bank of LEDs. As a first check, verify that the LAN Link and ADSL line LEDs are lit. If they are not, verify that you are using the proper cables.

Chapter 3
Configuration

The ADSL Wireless Router can be configured with your Web browser. The web browser is included as a standard application in the following operation systems, UNIX, Linux, Mac OS, Windows 95/98/NT/2000/Me, and etc. The product provides a very easy and user-friendly interface for configuration.

3.1 Before Configuration

This section describes the configuration required by LAN-attached PCs that communicate with the ADSL Wireless Router, either to configure the device or for network access. These PCs must have an Ethernet interface (or wireless adapter) installed properly, be connected to the ADSL Wireless Router either directly or through an external repeater hub, and have TCP/IP installed and configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet of the ADSL Firewall Router. The default IP address of the ADSL Wireless Router is 192.168.1.254 and subnet mask is 255.255.255.0. The best and easy way is to configure the PC to get an IP address from the ADSL Wireless Router. Also make sure you have UNINSTALLED any kind of software firewall that can cause problems while accessing the 192.168.1.254 IP address of the router.
Please follow the steps below for PC's network environment installation. First of all, please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to MS Windows related manuals.

Any TCP/IP capable workstation can be used to communicate with or through the ADSL Wireless Router. To configure other types of workstations, please consult the manufacturer's documentation.

3.2 Connecting the I-Fly Wireless Router ADSL

- Connect the Router to a LAN (Local Area Network) and the ADSL/telephone network.
- Power on the device
- Make sure the PWR and SYS LEDs are lit steady & LAN/WLAN LED is lit.
- Before taking the next step, make sure you have uninstalled any software firewall.

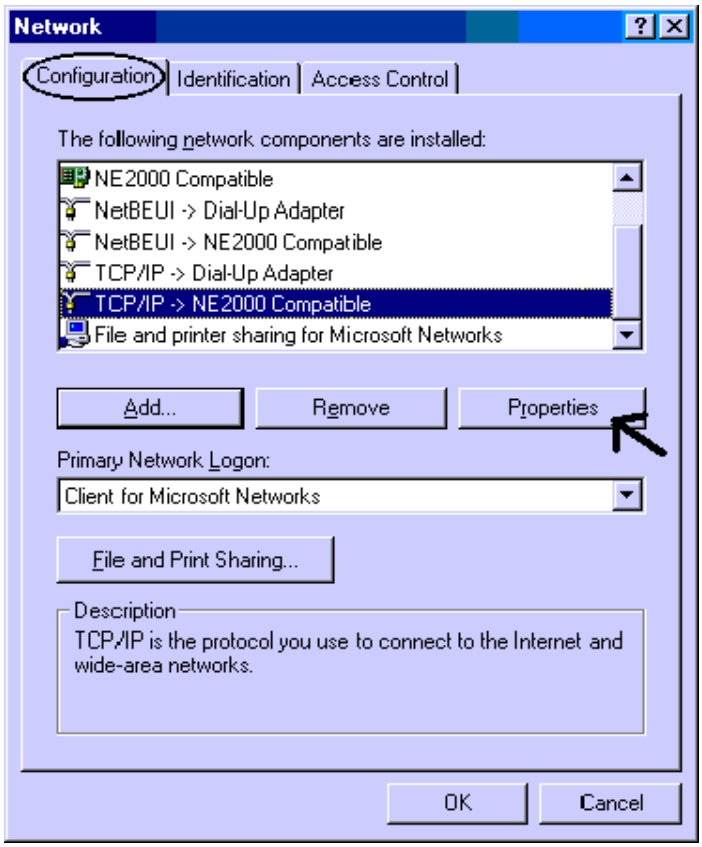
3.3 Configuring PC in Windows

For Windows 95/98/ME

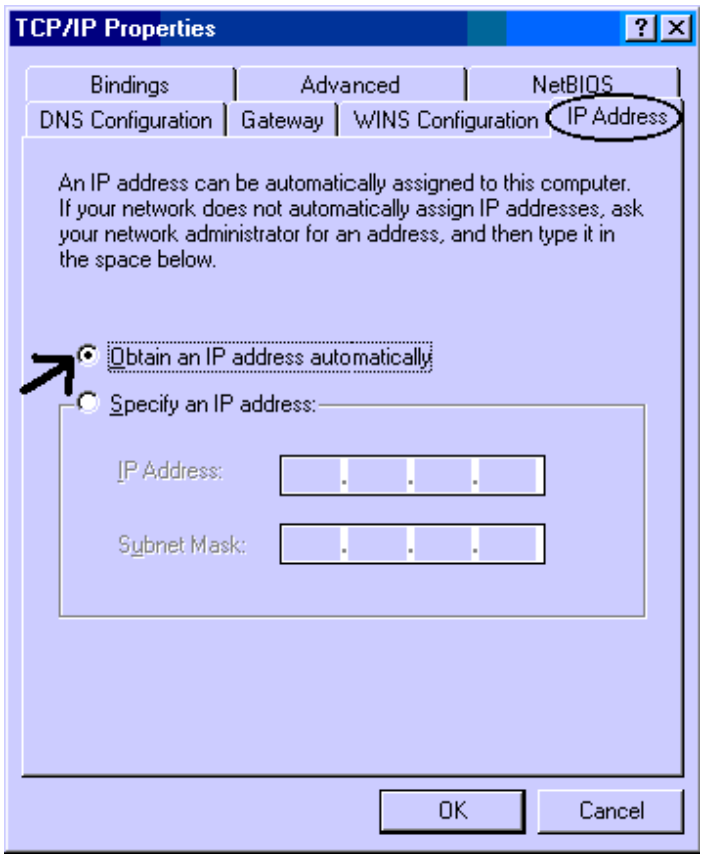
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.

2. Select **TCP / IP -> NE2000 Compatible**, or the name of any Network Interface Card (NIC) in your PC.

3. Click Properties.

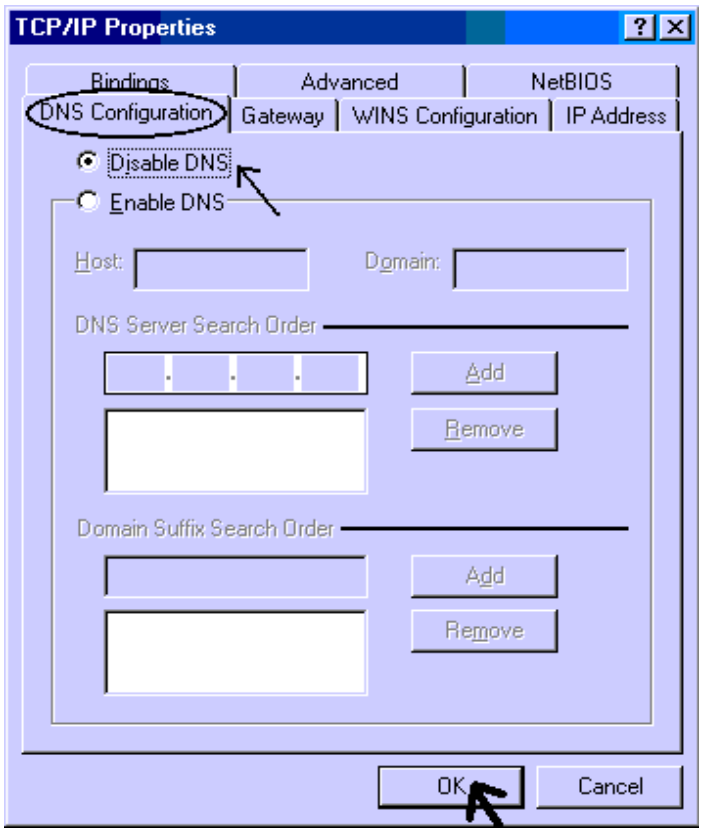


4. Select the **IP Address** tab. In this page, click the **Obtain an IP address automatically** radio button.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

5. Then select the **DNS Configuration** tab.

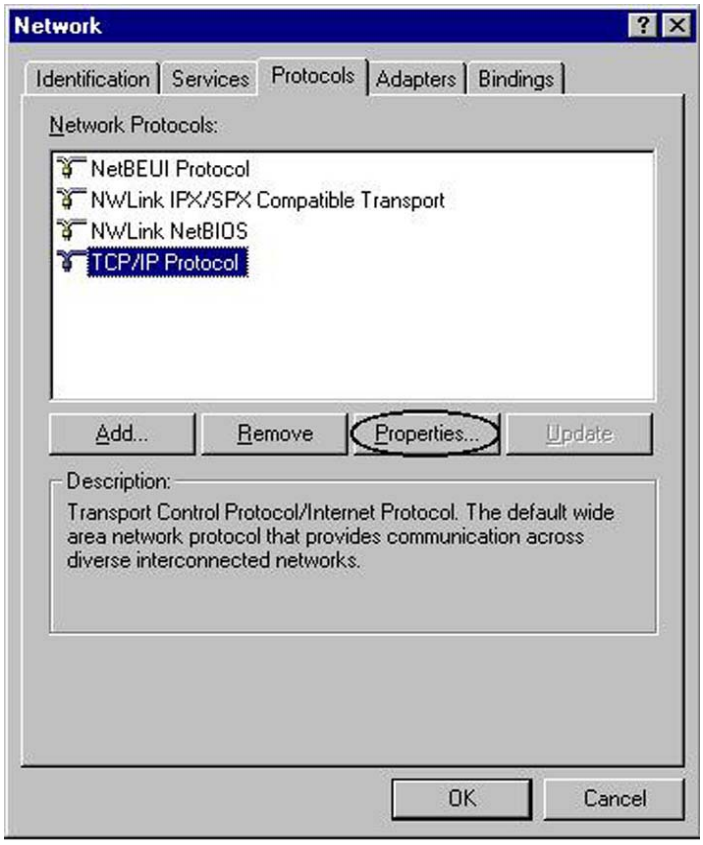
6. Select the **Disable DNS** radio button and click **"OK"** to finish the configuration.



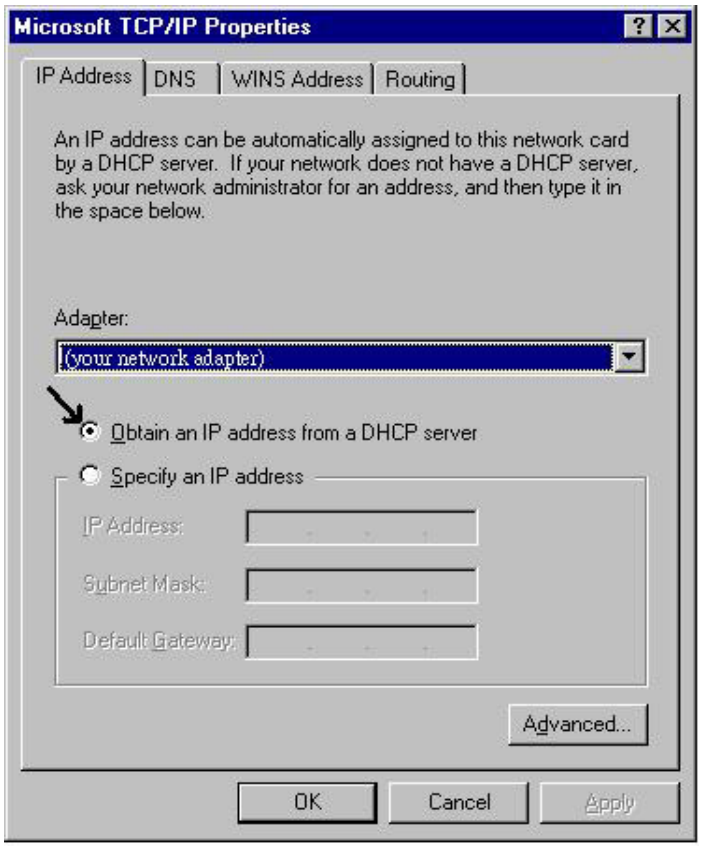
For Windows NT4.0

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Protocols** tab.

2. Select **TCP/IP Protocol** and click **Properties**.



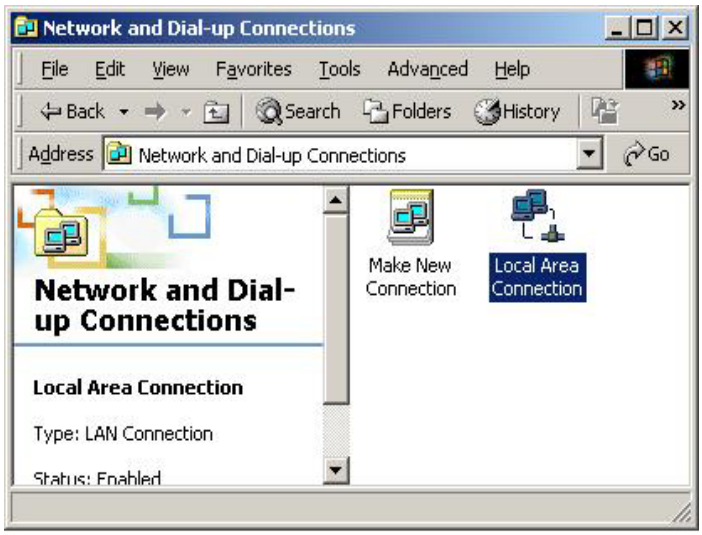
3. Select the **Obtain an IP address from a DHCP server** radio button and click **"OK"**.


Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
(your network adapter)
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

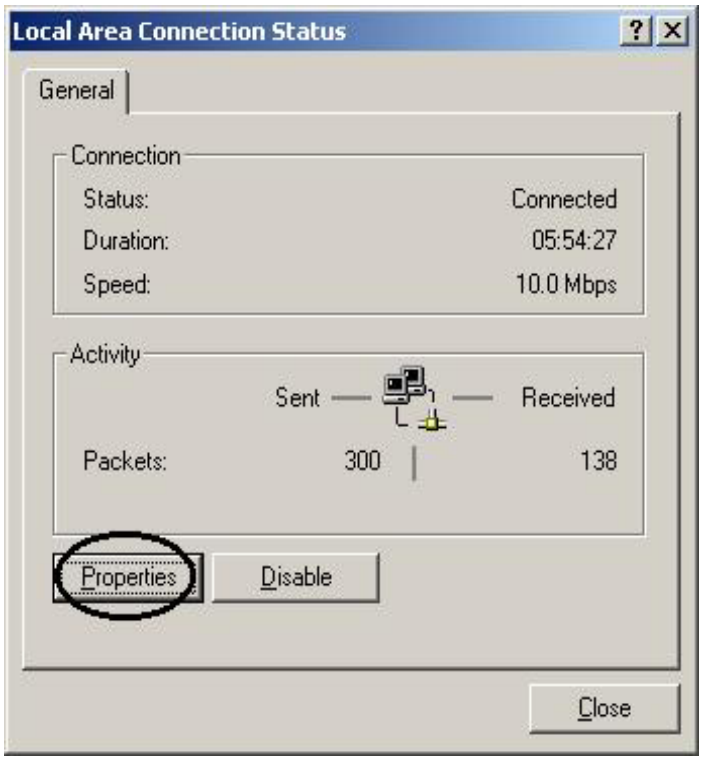
For Windows 2000

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.

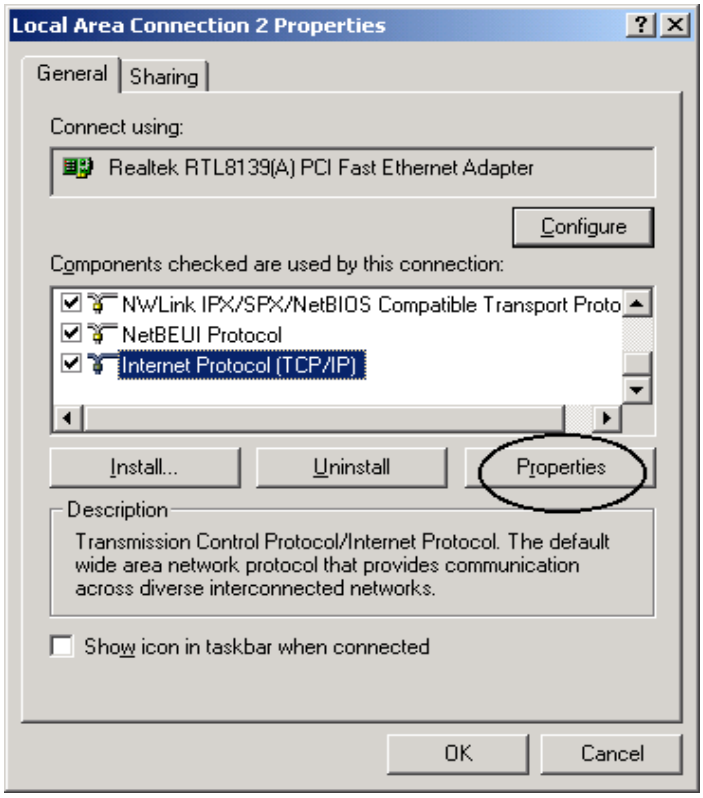
2. Double-click **LAN Area Connection**.



3. In the **LAN Area Connection Status** window, click **Properties**.

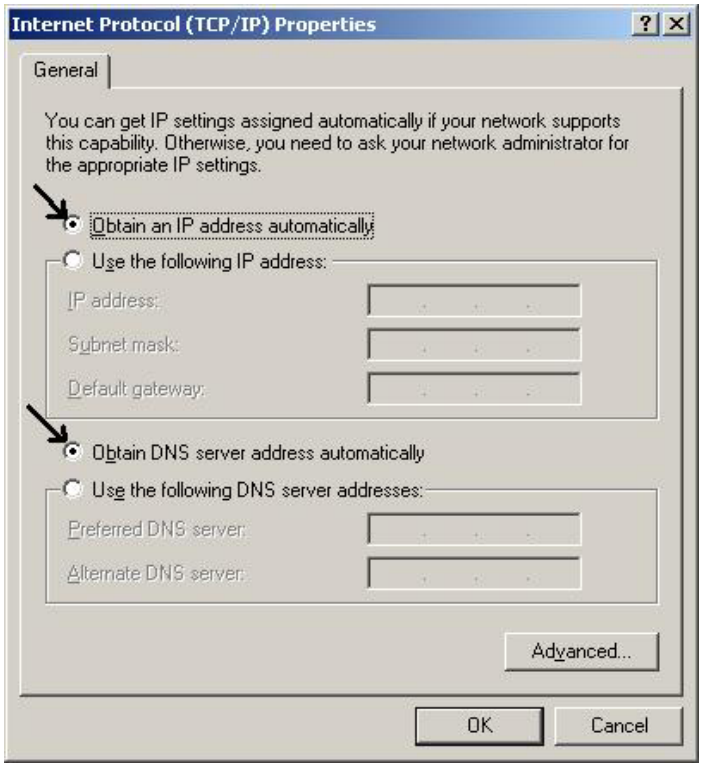


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

6. Click **"OK"** to finish the configuration.

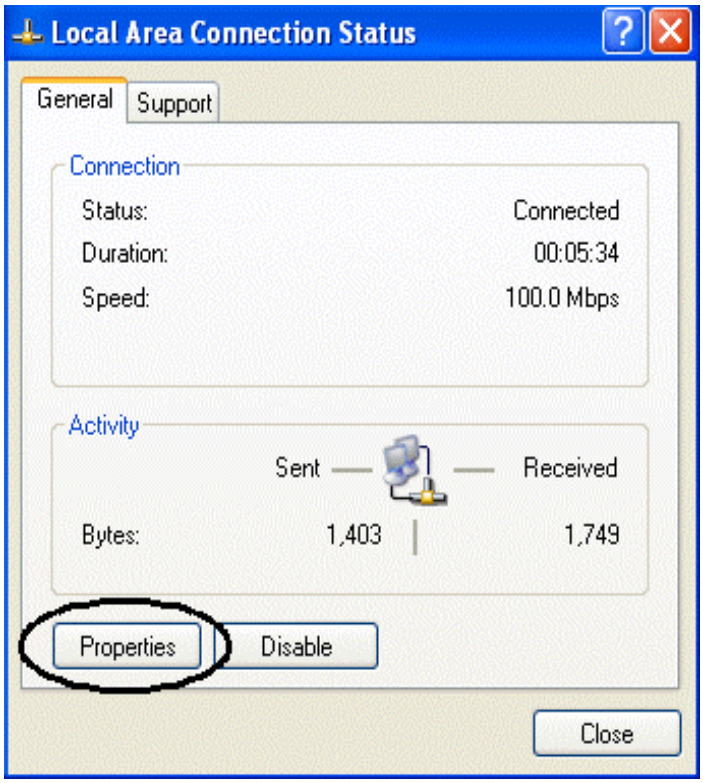

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

For Windows XP

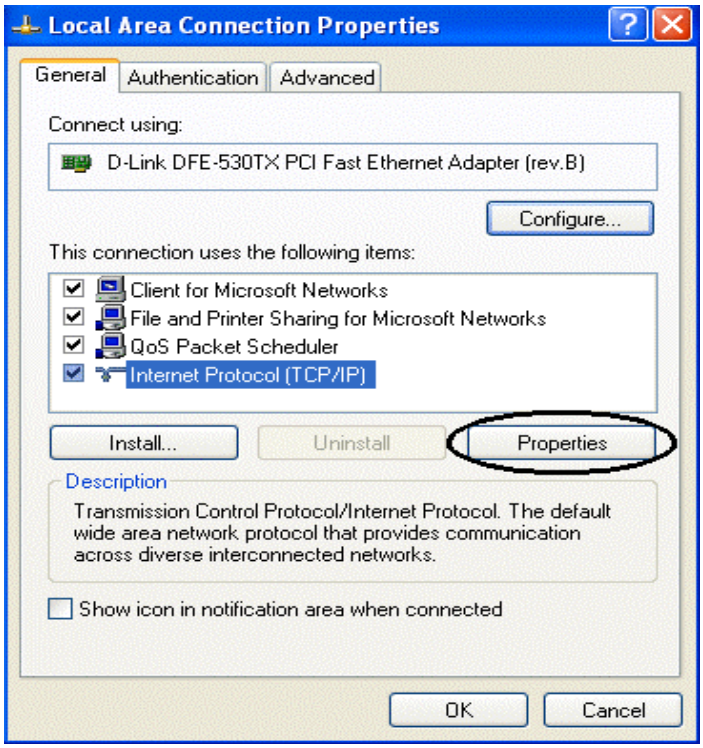
1. Go to **Start / Control Panel** (in Classic View). In the Control Panel, double-click on **Network Connections.**

2. Double-click **Local Area Connection**

3. In the **LAN Area Connection Status** window, click **Properties**.

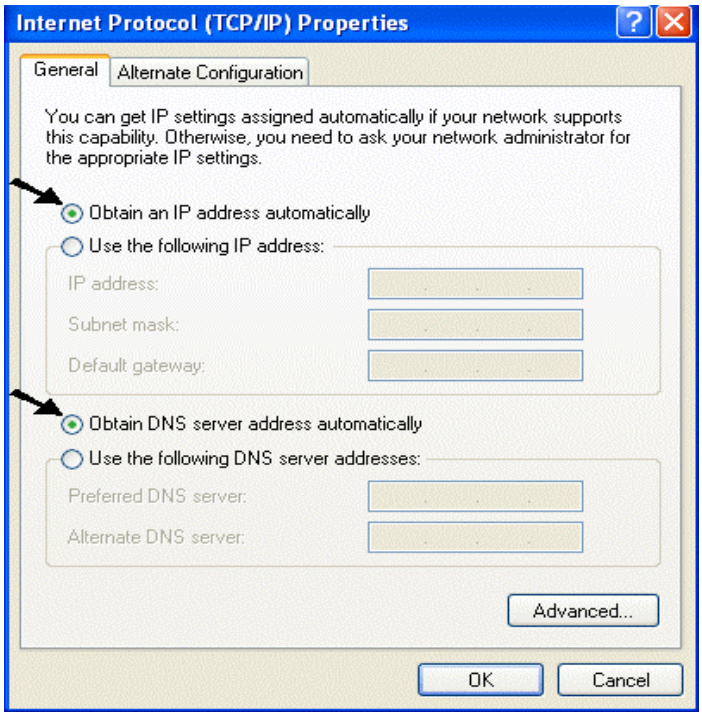


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons

6. Click **"OK"** to finish the configuration.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

3.4 Factory Default Settings

Before configurating this ADSL Wireless Router, you need to know the following default settings.

- Username: **admin**
- Password : **atlantis**
- IP Address : **192.168.1.254**
- Subnet Mask : **255.255.255.0**
- DHCP server is enabled.
- Wireless**:** SSSID= **wlan-ap**, Channel=**6**, WEP=**disable**

3.4.1 Username and Password

The default username and password are **admin** and **atlantis** respectively.

If you ever forget the password to log in, you may press the RESET button to restore the factory default settings..

3.4.2 LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown below.

LAN Port		WAN Port
IP address	192.168.1.254	N/A
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	

3.5 Information from the ISP

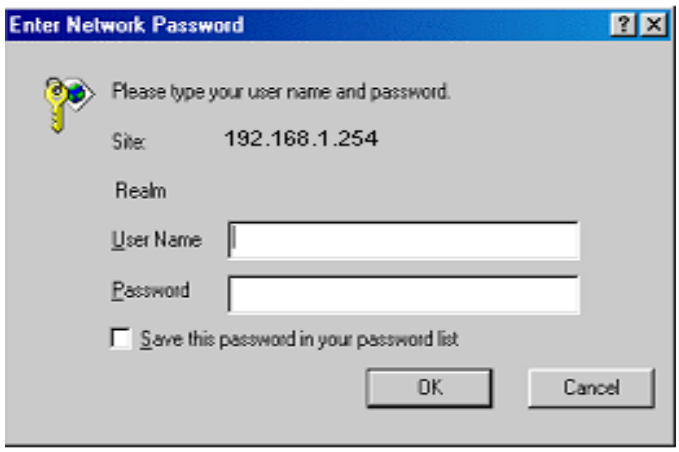
Before configuring this device, you have to check with your ISP (Internet Service Provider) what kind of service is provided such as PPPoE, PPPoA, RFC1483, IPoA, or PPTP-to-PPPoA Relaying.

Gather the information as illustrated in the following table and keep it for reference.

PPPoE	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed).
PPPoA	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, and Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed).
RFC1483 Bridged	VPI/VCI, VC-based/LLC-based multiplexing and configure this product into BRIDGE Mode.
RFC1483 Routed	VPI/VCI, VC-based/LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).
IPoA	VPI/VCI, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).

3.6 Configuring with the Web Browser

Open the web browser, enter the local port IP address of this ADSL Wireless Router, which defaults at **http://192.168.1.254**, and click "**Go**", a username and password window will appear. The default **username** & **password** are **admin** & **atlantis**, in respectively



You will get a status report web page when login successfully.

At the configuration homepage, the left navigation page where bookmarks are provided links you directly to the desired setup page, including:

- **Status** (ARP Table,Routing Table, DHCP Table, PPTP Status, Email Status, Event Log & Error Log)
- **Quick Start**
- **Configuration** (LAN, WAN, System, Firewall, VPN, QoS, Virtual Server & Advanced)
- **Save Config to FLASH**
- **Language** (provides user interface in multi-languages).

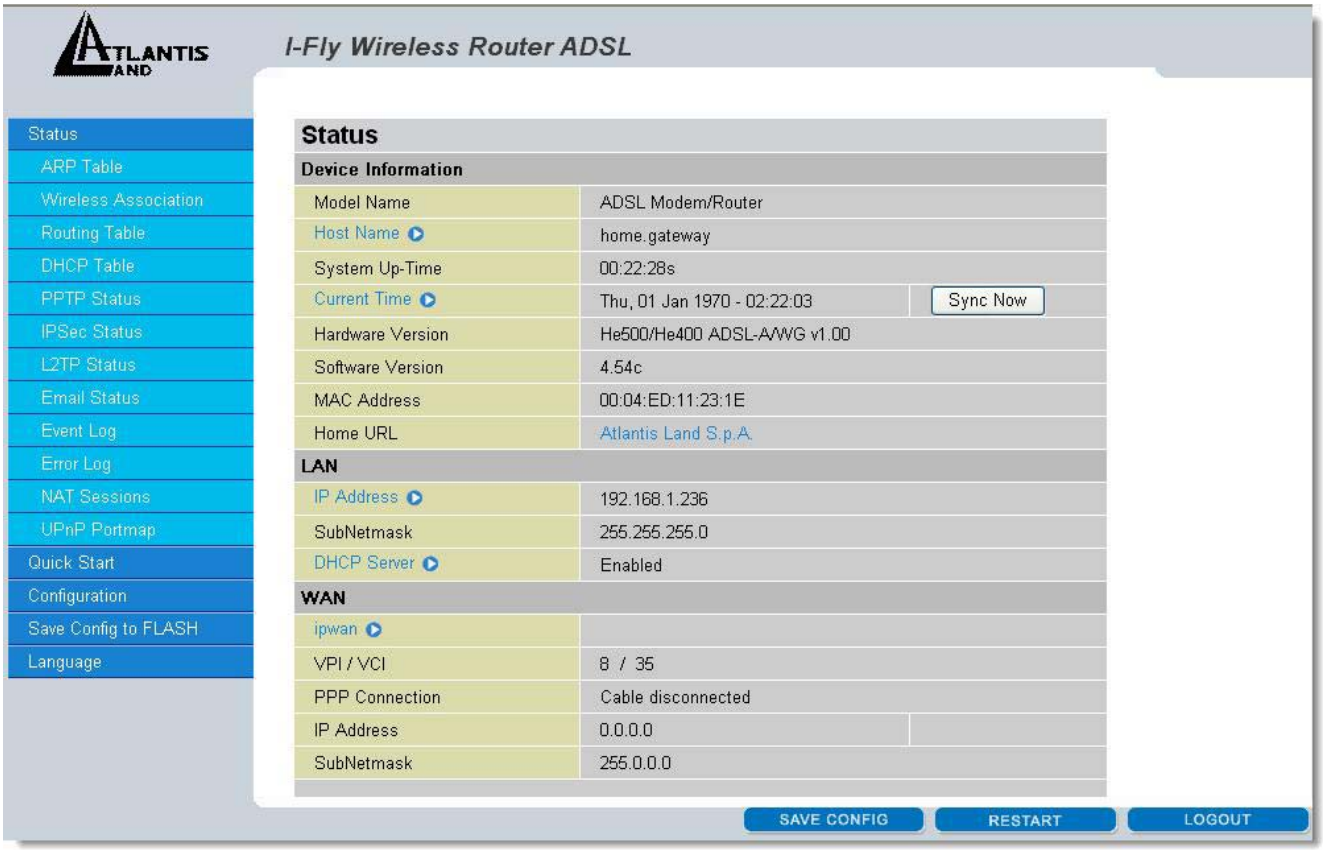
Click on the desired item to expand the page in the main navigation page.

3.6.1 STATUS

Status section provides and contains many items including device H/W and S/W information, LAN, WAN, Port status and all defined interfaces. It also provides various and useful information for user to exam the status of the device.

- **ARP Table**
- **Wireless Association**
- **Routing Table**
- **DHCP Table**
- **PPTP Status**

- **IPSec Status**
- **L2TP**
- **Email Status**
- **Event Log**
- **Error Log**
- **NAT Sessions**
- **UPnP PortMap**



When you click the **ARP Table,** you will see the data of the IP address of each PC in your LAN as well as its associated MAC address.

When you click the **DHCP Table,** you can see the status of the assigned IP addresses with its associated information.

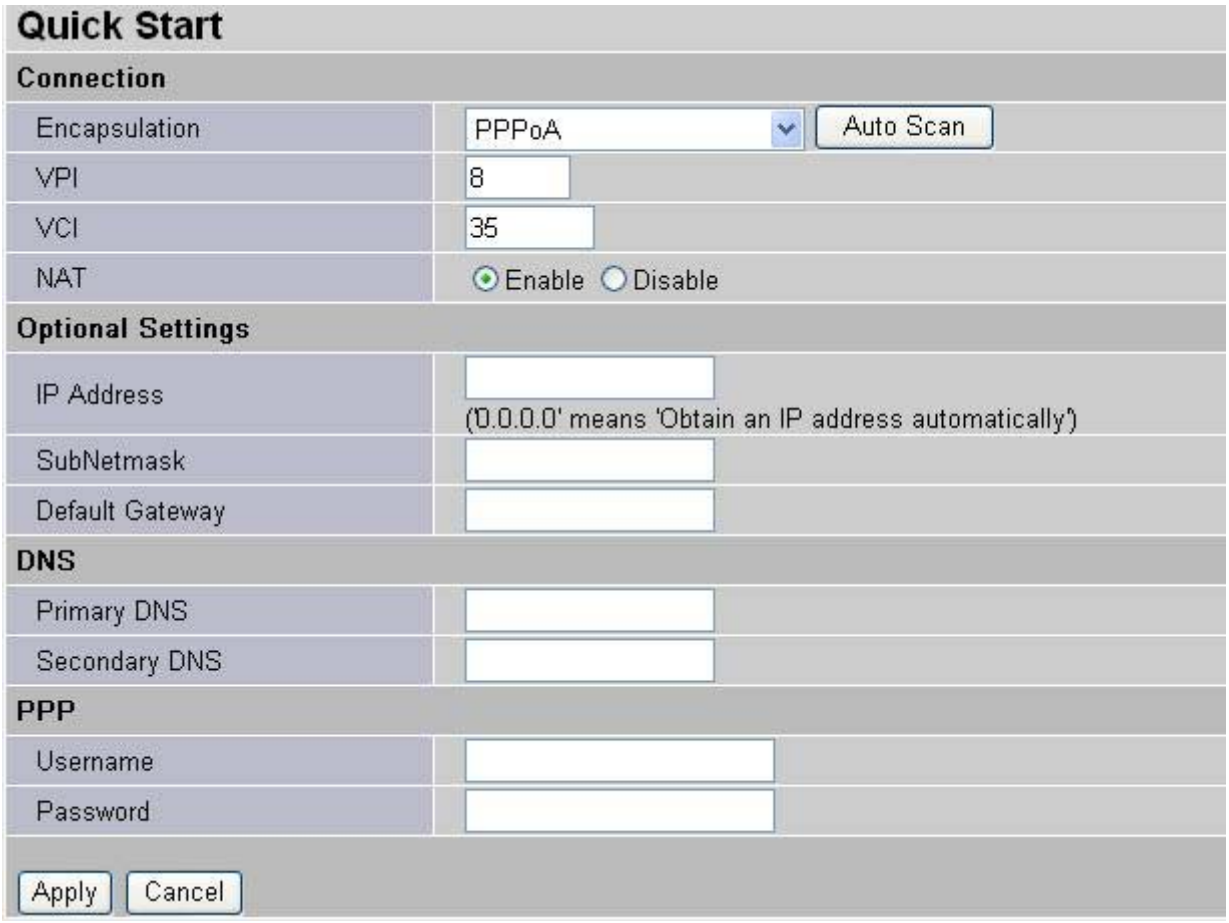
When you click the **PPTP Status**, it gives you a quick view to know the ADSL Router's current status. The status of PPTP connection will be shown.

When you click the **Email Status**, it gives you a quick view to know if there is email in your pre-defined email account. You will see the unread emails in the email server and, once you have configured successfully the "Check Emails" in **Configuration → Advance.**

When you click the **Event Log**, it displays the valuable system event logging information and status after the power is turned on, such as ADSL line, WAN port, SNTP, Firewall, and etc.

When you click the **Error Log**, it shows the error message log. When you face a problem, please send this error log to support for a quick feedback.

3.6.2 Quick Start



If you use this device to access the Internet through the ISP, this web page is enough for you to configure this router and access the Internet without a problem. Please check Chapter 3.5 (*Information from the ISP)*, then enter the proper values into this web page, click the **Apply** button and then **Save Config to FLASH** in the left panel. After the router reboot, you may check the Status web page to check whether the router is connected to the ISP or not. In most cases, you can access the Internet immediately. If not, please refer to the sections below for more information.

3.6.3 Configuration

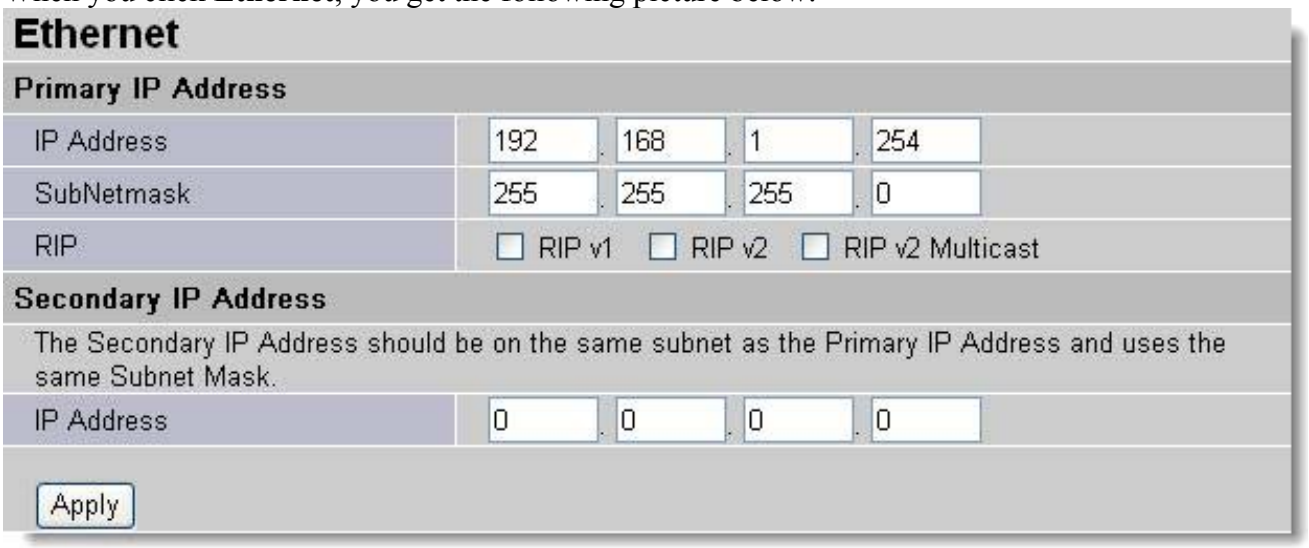
When you click this item, you get following sub-items to configure the ADSL router.
LAN, WAN, System, Firewall, VPN, QoS,Virtual Server and Advanced
These functions are described below in the following sections.

3.6.3.1 LAN

There are four items within the LAN section: **Ethernet, Wireless, Wireless Security, Port Setting** and **DHCP Server.**

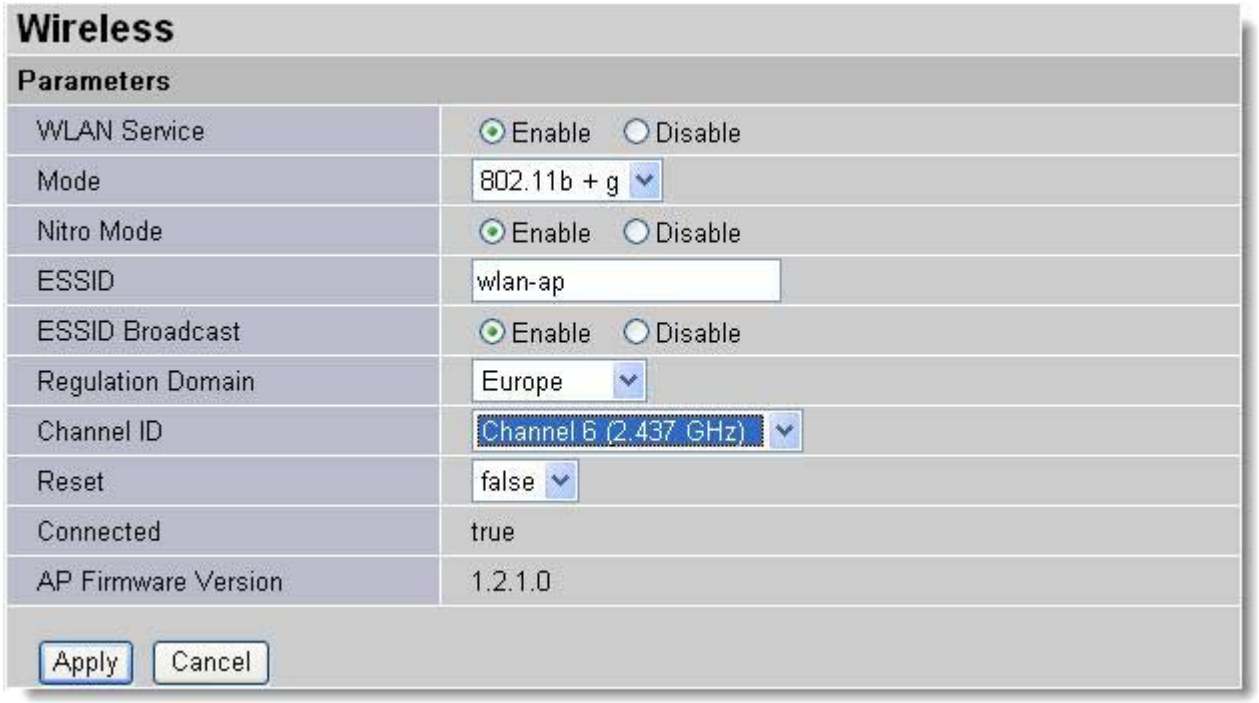
3.6.3.1.1 Ethernet

When you click **Ethernet**, you get the following picture below.


Ethernet
Primary IP Address
IP Address
192 . 168 . 1 . 254
SubNetmask
255 . 255 . 255 . 0
RIP
RIP v1
RIP v2
RIP v2 Multicast
Secondary IP Address
The Secondary IP Address should be on the same subnet as the Primary IP Address and uses the same Subnet Mask.
IP Address
0 . 0 . 0 . 0
Apply

It supports two Ethernet IP addresses in the LAN. With this function, the ADSL Wireless router can support two different IP. Usually, there is only one subnet in LAN and no need to configure a Secondary IP address. The 192.168.1.254 is the default IP address for this ADSL Wireless router.
RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

3.6.3.1.2 Wireless



WLAN Service: Default setting is set to Enable.
Mode: The factory default is 802.11b + g.

- 802.11b + g (Mixed mode)
- 802.11b
- 802.11g

Nitro Mode: Default is enabled for increasing performance in mixed 802.11b and 802.11g wireless networks.

ESSID: Enter the unique ID given to the Access Point (AP), which is already built-in to the router's wireless interface. To connect to this device, your wireless clients must have the same ESSID as the device.

ESSID Broadcast:

- **Disable:** Any client that using the "any" setting cannot discover the Access Point (AP) in question.
- **Enable:** Any client that using the "any" setting can discover the Access Point (AP) in question.

Regulation Domain: There are five Regulation Domains for you to choose from, including **North America (N.America)**, **Europe**, **France**, etc. The Channel ID will be different based on this setting.

Channel ID: Select the ID channel that you would like to use.

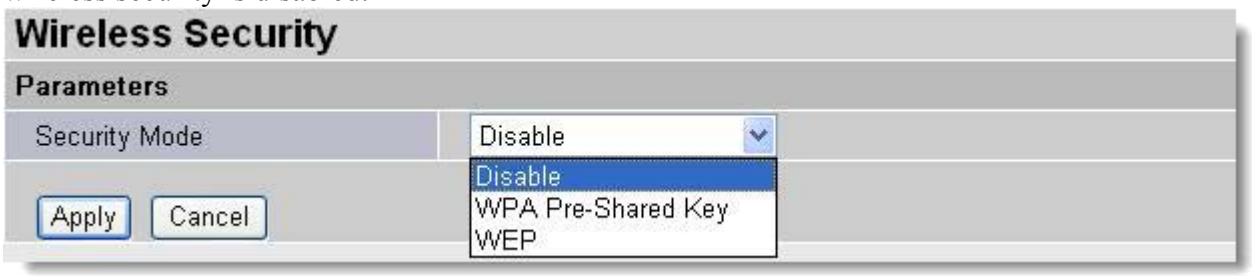
Reset: Reset the Access Point (AP), which is already built-in to the router's wireless interface.

Connected: true or false. That it is the connection status between the system and the build-in wireless card.

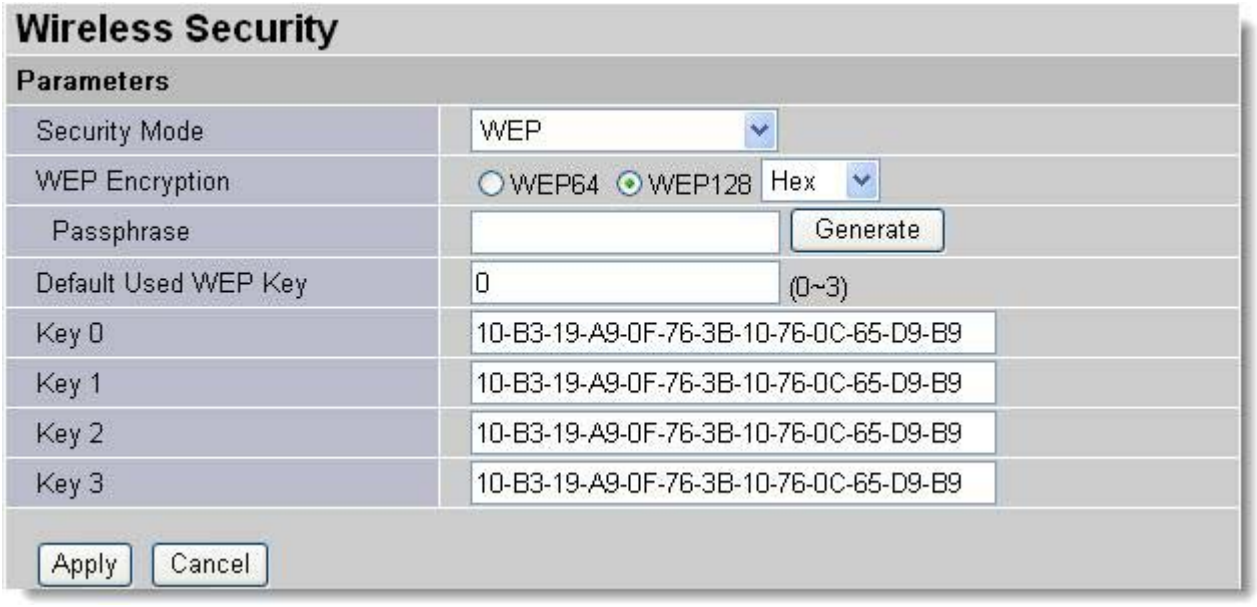
AP Firmware Version: The Access Point firmware version.

3.8.2.1.3 Wireless Security

You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is disabled.



- **WEP**

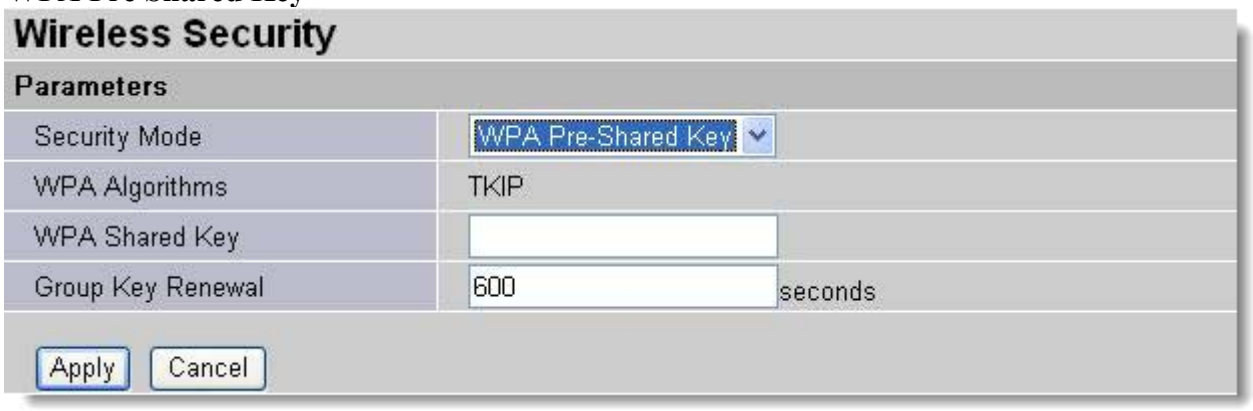


WEP Encryption: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers highly secure data encryption, known as WEP. If you require high security for transmissions, there are two alternatives to select from: WEP 64 and WEP 128. WEP 128 will offer increased security over WEP 64.

Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128. You can input the same string in both the AP

and Client card settings to generate the same WEP keys. Please note that you do not have to enter Key (0-3) as below when the Passphrase is enabled.
Default Used WEP Key: Select the encryption key ID, please refer to Key (0-3) below.
Key (0-3): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router.
There are four keys for your selection. The input format is in HEX [0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F] style, 5 and 13 HEX codes are required for WEP64 and WEP128 respectively, the separator is "-".

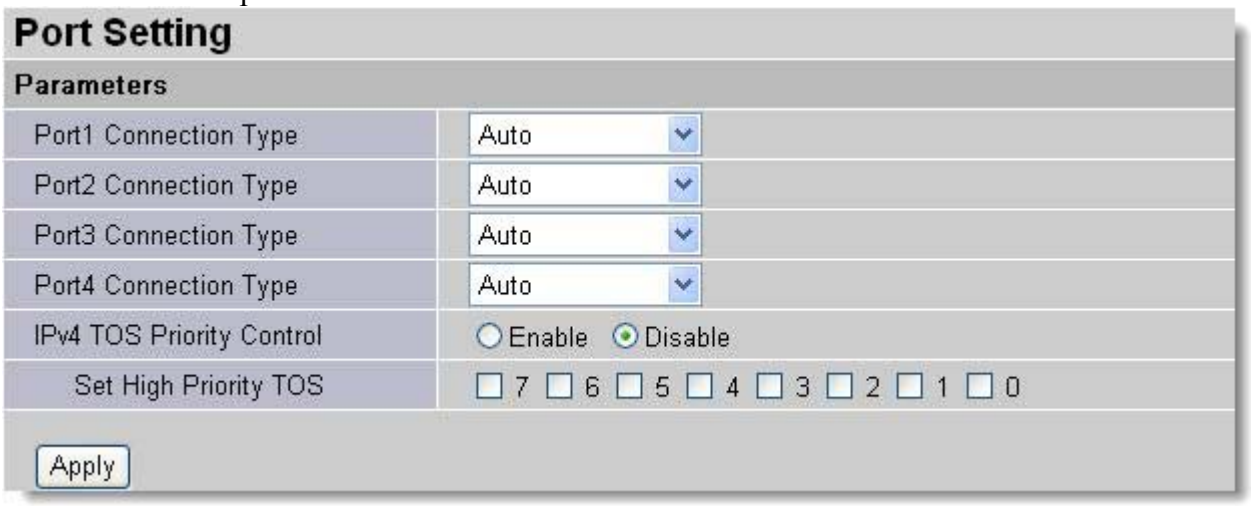
- **WPA Pre Shared Key**



WPA Algorithms: TKIP (Temporal Key Integrity Protocol) utilizes a stronger encryption method and incorporates Message Integrity Code (**MIC**) to provide protection against hackers.
WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.
Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP).

3.6.3.1.4 Port Settings

This section allows you to configure the settings for the router's Ethernet ports to solve some of the compatibility problems that may be encountered while connecting to the Internet, as well allowing users to tweak the performance of their network.



Port # Connection Type: Five options to choose from: Auto, 10M half-duplex, 10M fullduplex, 100M half-duplex or 100M full-duplex. Sometimes, there are Ethernet compatibility problems with legacy Ethernet devices, and you can configure different types to solve compatibility issues. The

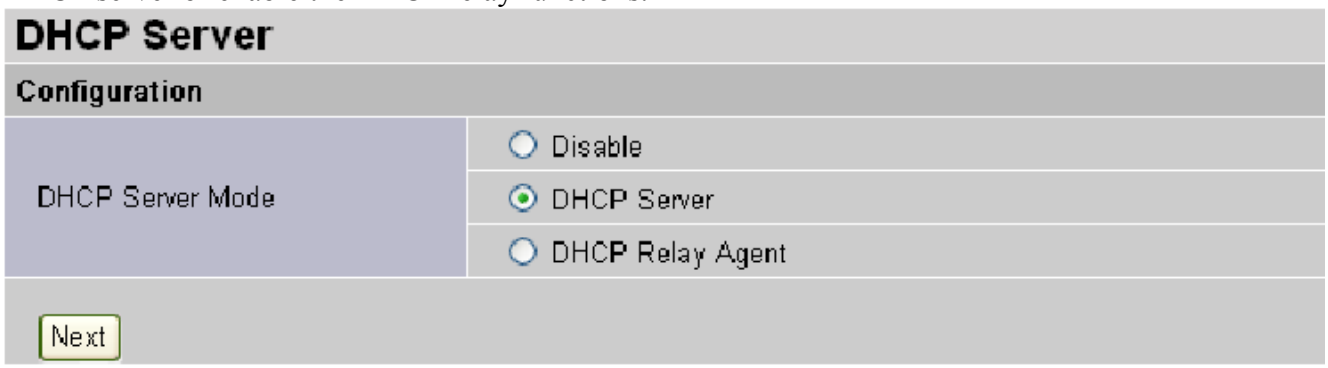
default is Auto, which users should keep unless there are specific problems with PCs not being able to access your LAN.

IPv4 TOS priority Control (Advanced users): TOS, Type of Services, is the 2nd octet of an IP packet. Bits 6-7 of this octet are reserved and bit 0-2 are used to specify the priority (precedence) of the packet, and bits 3-5 are specified the delay, throughput and reliability.

This feature uses bits 0-2 to classify the packet's priority. If the packet is high priority, it will flow first. Therefore, when this feature is enabled, the router's Ethernet switch will check the 2nd octet of each IP packet. If the value in the Precedence of TOS field matches the checked values in the table (0 to 7), this packet will be treated as high priority.

3.6.3.1.5 DHCP

When you click **DHCP Server**, you will get the following figure. You can disable or enable the DHCP server or enable the DHCP relay functions.



If you check **Disabled** and click **Next,** then click **Apply.** The DHCP server function is disabled. Each PC in the LAN should assign a fixed IP address and set the PC's gateway to the ADSL Router.

If you check **DHCP Server** and click **Next**, you can configure parameters of the DHCP server including the IP pool (starting IP address and ending IP address), leased time for each assigned IP address, DNS IP address, and Gateway IP address. Those messages are sent to the DHCP client when it requests an IP address from the DHCP server. Click **Apply** to enable this function. If you check "Use Router as a DNS Server", the ADSL Router will find the IP address from the outside network automatically and forward it back to requesting PC in the LAN.

If you check **DHCP Relay Agent** and click **Next**, then you will have to enter the IP address of the DHCP server, which will assign an IP address back to the DHCP client in the LAN. Click **Apply** to enable this function.

DHCP Server

⊙ **Disable:** Check to disable the ADSL Firewall Router from distributing IP Addresses to the local network.

If you check this selection, remember to specify a static IP address, subnet Mask, and DNS setting for each of your local computers. Be careful NOT to assign the same IP address to different computers.

⊙ **DHCP Server:** Check to enable the ADSL Firewall Router to distribute IP Addresses, subnet mask and DNS setting to computers. Hence, the following fields will be activated.

Starting IP Address: Enter the starting address of this local IP network address pool. The pool is a piece of continuous IP address segment. The default value is **192.168.1.100**.

Ending IP Address: Enter the ending address of this local IP network address pool. The pool is a piece of continuous IP address segment. The default value is **192.168.1.199**

Defaul Lease Time: Value that expresses in second the validity time of assigned address.

Maximum Lease Time: Value that expresses in second the maximum validity time of assigned address.

Use Router as DNS Server: Each DNS request will be received by router and forwarder to DNS Server

Primary/Secondary DNS Server Address: Insert here remote DSN server addresses, it will be forwarded to LAN hosts by DHCP server.

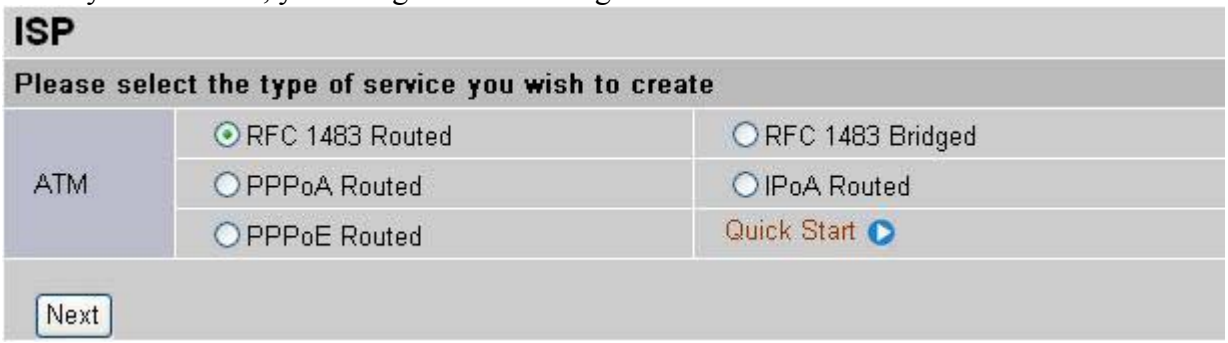
Use Router as Default Gateway: Specify here which address will be used by LAN hosts as Default Gateway
DHCP Relay: Selecting this option the DHCP request performed by LAN host will by delivered by a remote DHCP server passing through ADSL Firewal Router.

3.6.3.2 WAN

There are two items under the WAN section, ISP, DNS and ADSL.

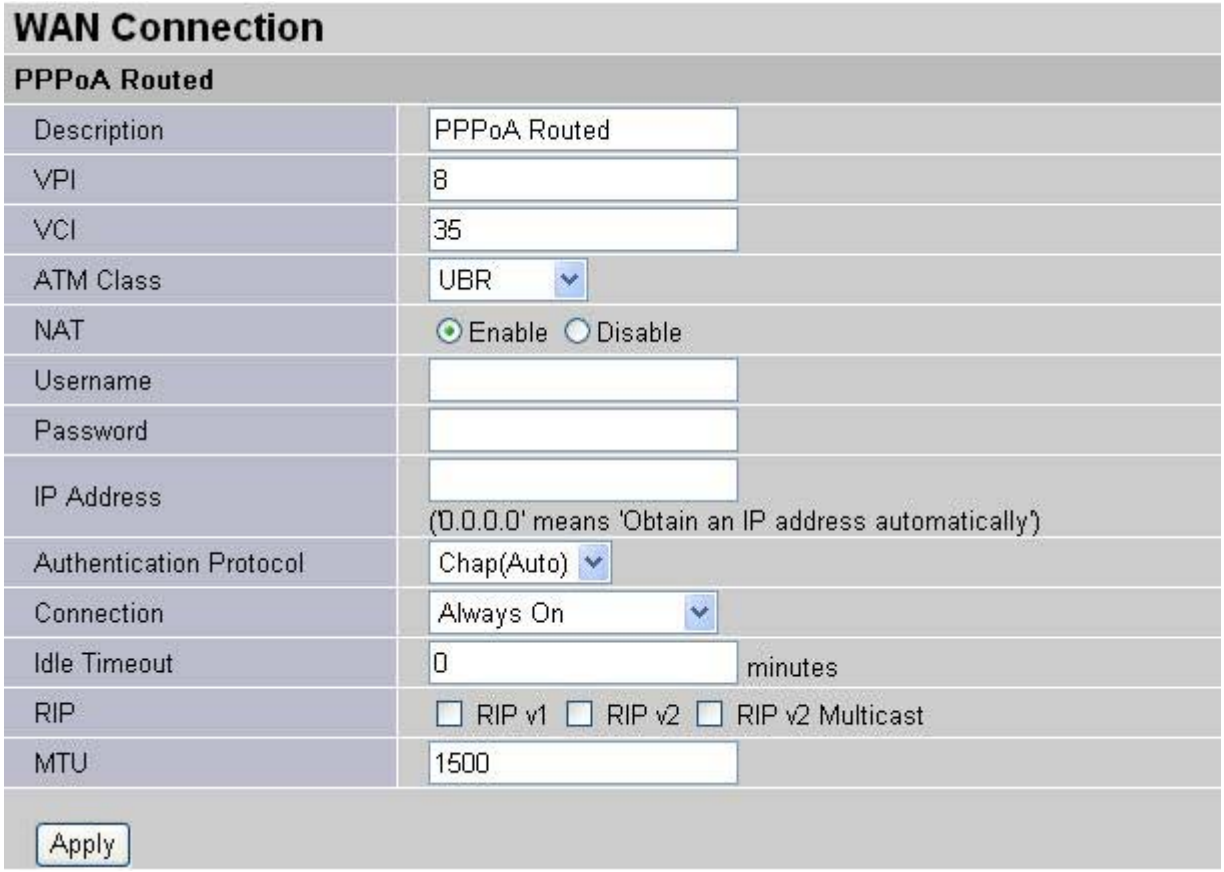
3.6.3.2.1 ISP

Check one of the access methods among the 5 listed items and clicks **Next** to configure the right connection method.
When you click **ISP**, you will get the following screen.



The factory default is PPPoE mode. If your ISP uses the same access protocol, please click **Edit** to input other parameters as below. If your ISP does not use PPPoE mode, you can delete it, click **Delete**. Then you may click **Create** to create a connection to your ISP to surf the Internet. Refer to the figure after the PPPoE mode description below.

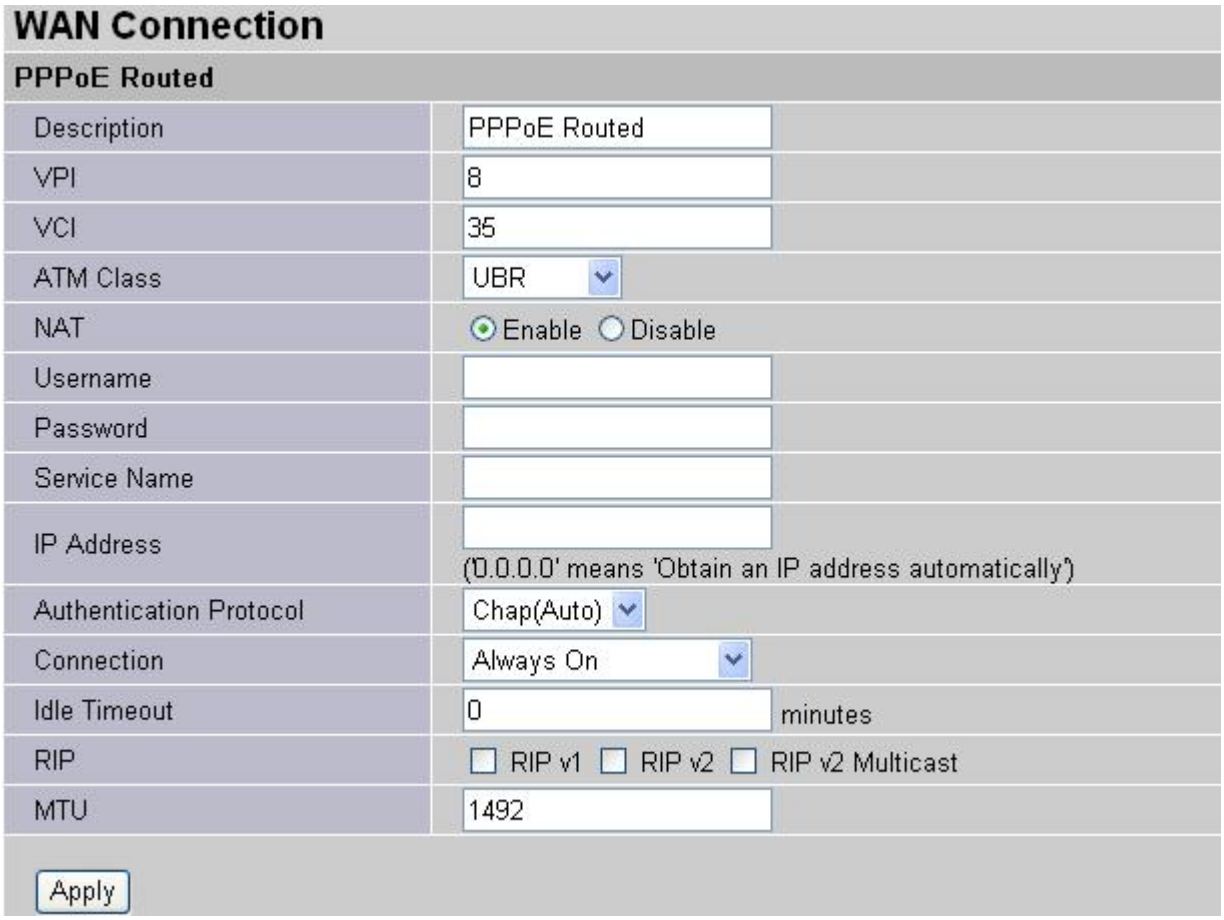
- **PPPoA**



Description: User-definable name for the connection.
VPI/VCI: Enter the information provided by your ISP.
ATM Class: The Quality of Service for ATM layer.
NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.
Username: Enter the username provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive). This will usually be in the format of "username@ispname" instead of simply "username".
Password: Enter the password provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive).
IP Address: Specify an IP address allowed to logon and access the router's web server.
Note: IP 0.0.0.0 indicates all users who are connected to this router are allowed to logon the device and modify data.
Authentication Protocol Type: Default is Chap (Auto). Your ISP will advise you whether to use Chap or Pap.
Always on: If you want the router to establish a PPPoA session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.
Connect to Demand: If you want to establish a PPPoA session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).
Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.
Detail: You can define the destination port and packet type (TCP/UDP) without checking by timer. It allows you to set which outgoing traffic will not trigger and reset the idle timer.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.
MTU: Maximum Transmission Unit. The size of the largest datagram (excluding mediaspecific headers) that IP will attempt to send through the interface.

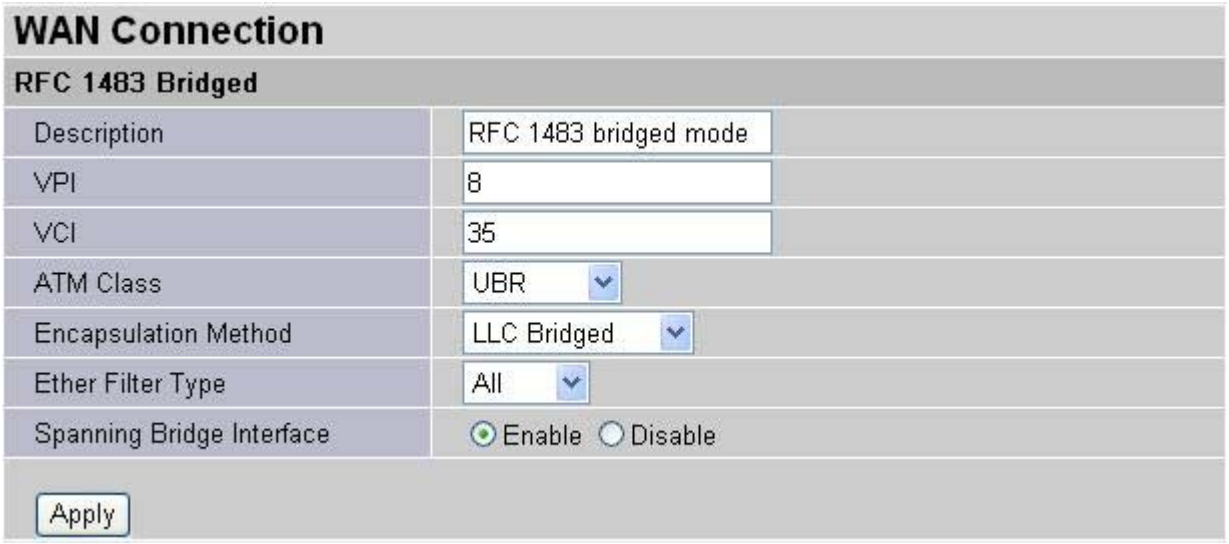
- **PPPoE Routed**



Description: User-definable name for the connection.
VPI/VCI: Enter the information provided by your ISP.
ATM Class: The Quality of Service for ATM layer.
NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.
Username: Enter the username provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive). This will usually be in the format of "username@ispname" instead of simply "username".
Password: Enter the password provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive).
Service Name: This item is for identification purposes. If it is required, your ISP will provide you the information. Maximum input is 20 alphanumeric characters.
IP Address: Specify an IP address allowed to logon and access the router's web server.
Note: IP 0.0.0.0 indicates all users who are connected to this router are allowed to logon the device and modify data.
Authentication Protocol Type: Default is Chap (Auto). Your ISP will advise you whether to use Chap or Pap.

Always on: If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.
Connect to Demand: If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).
Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.
Detail: You can define the destination port and packet type (TCP/UDP) without checking by timer. It allows you to set which outgoing traffic will not trigger and reset the idle timer.
RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.
MTU: Maximum Transmission Unit. The size of the largest datagram (excluding mediaspecific headers) that IP will attempt to send through the interface.

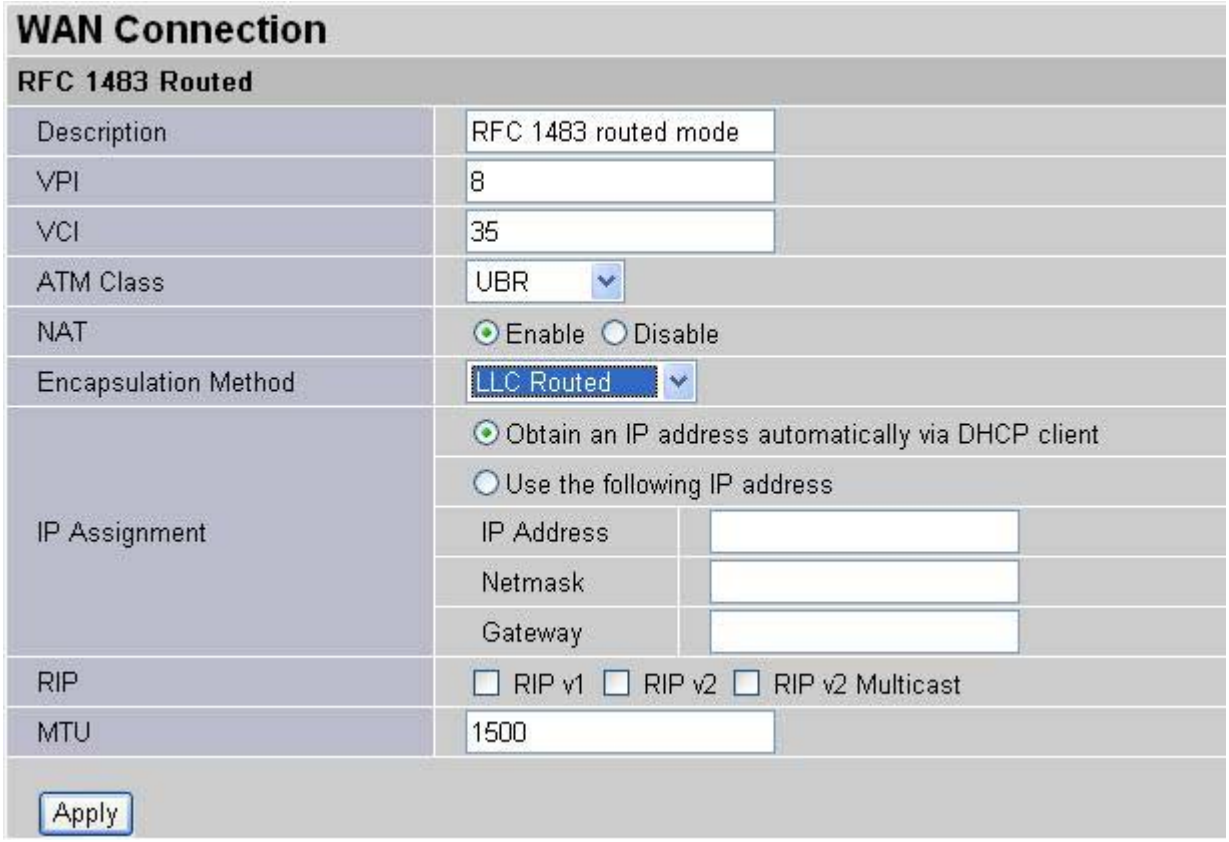
- **RFC 1483 Bridge**



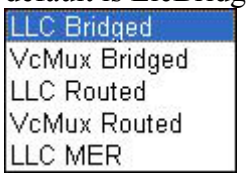
VPI and VCI: Enter the information provided by your ISP.
ATM Class: The Quality of Service for ATM layer.
Encapsulation method: Select the encapsulation format, this is provided by your ISP.
Ether Filter Type: Specify the type of ethernet filtering performed by the named bridge interface.
Spanning Bridge Interface: Enable/Disable spanning tree function of modem.
Ether Filter Type:

ALL	Allows all types of ethernet packets through the port.
IP	Allows only IP/ARP types of ethernet packets through the port.
PPPoE	Allows only PPPoE types of ethernet packets through the port.

- **RFC 1483 Routed/RFC1 1577(IPoA)**



Description: Your description of this connection.
VPI and VCI: Enter the information provided by your ISP.
ATM Class: The Quality of Service for ATM layer.
NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.
Encapsulation method (only for RFC 1483 Routed) : Select the encapsulation format, the default is LlcBridged. Select the one provided by your ISP.

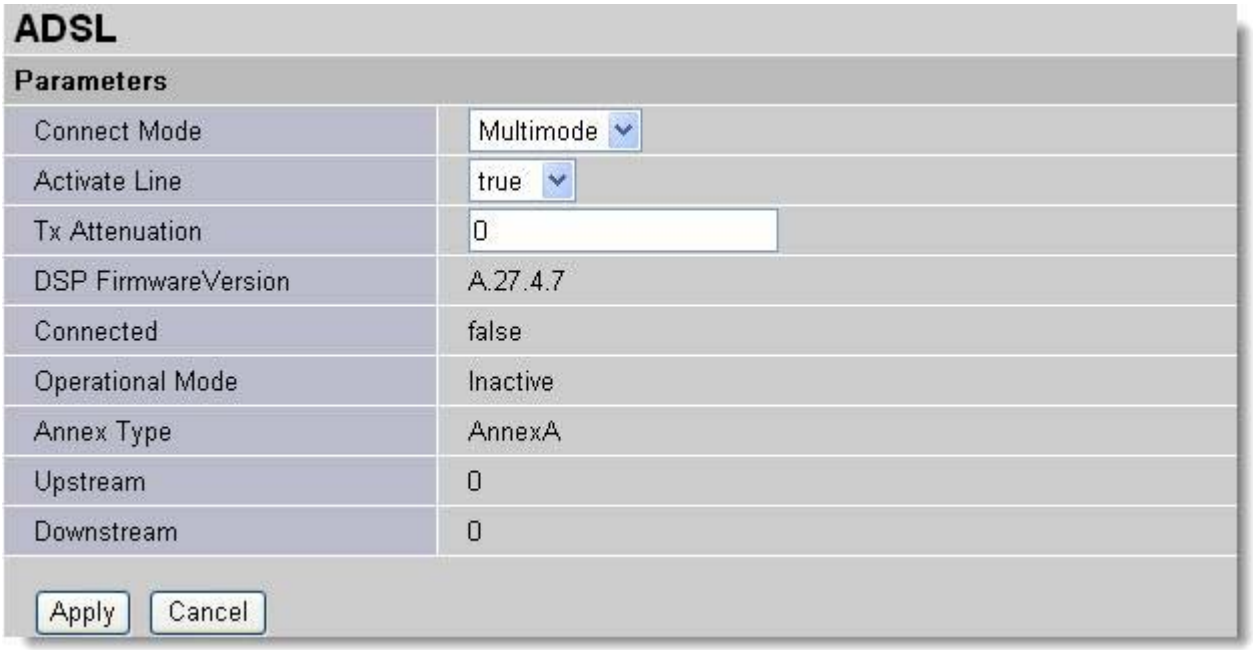


DHCP client: Enable or disable the DHCP client, specify if the Router can get an IP address from the Internet Service Provider (ISP) automatically or not. Please click **Obtain an IP address automatically via DHCP client** to enable the DHCP client function or click
Specify an IP address to disable the DHCP client function, and specify the IP address manually. The setting of this item is specified by your ISP.
RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.
MTU: Maximum Transmission Unit. The size of the largest datagram (excluding mediaspecific headers) that IP will attempt to send through the interface.

3.6.3.2.2 DNS

A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. In the Internet, every host has a unique and friendly name such as www.yahoo.com and an IP address. As the IP Address is hard to remember, the DNS converts the friendly name into its equivalent IP Address. You can obtain a Domain Name System (DNS) IP address automatically, if your ISP provides it when you logon. Usually when you choose PPPoE or PPPoA as your WAN - ISP protocol, the ISP will provide the DNS IP address automatically. You may leave it as blank. Or your ISP may provide you with an IP address of their DNS. If this is the case, you must enter the DNS IP address.

3.6.3.2.3 ADSL



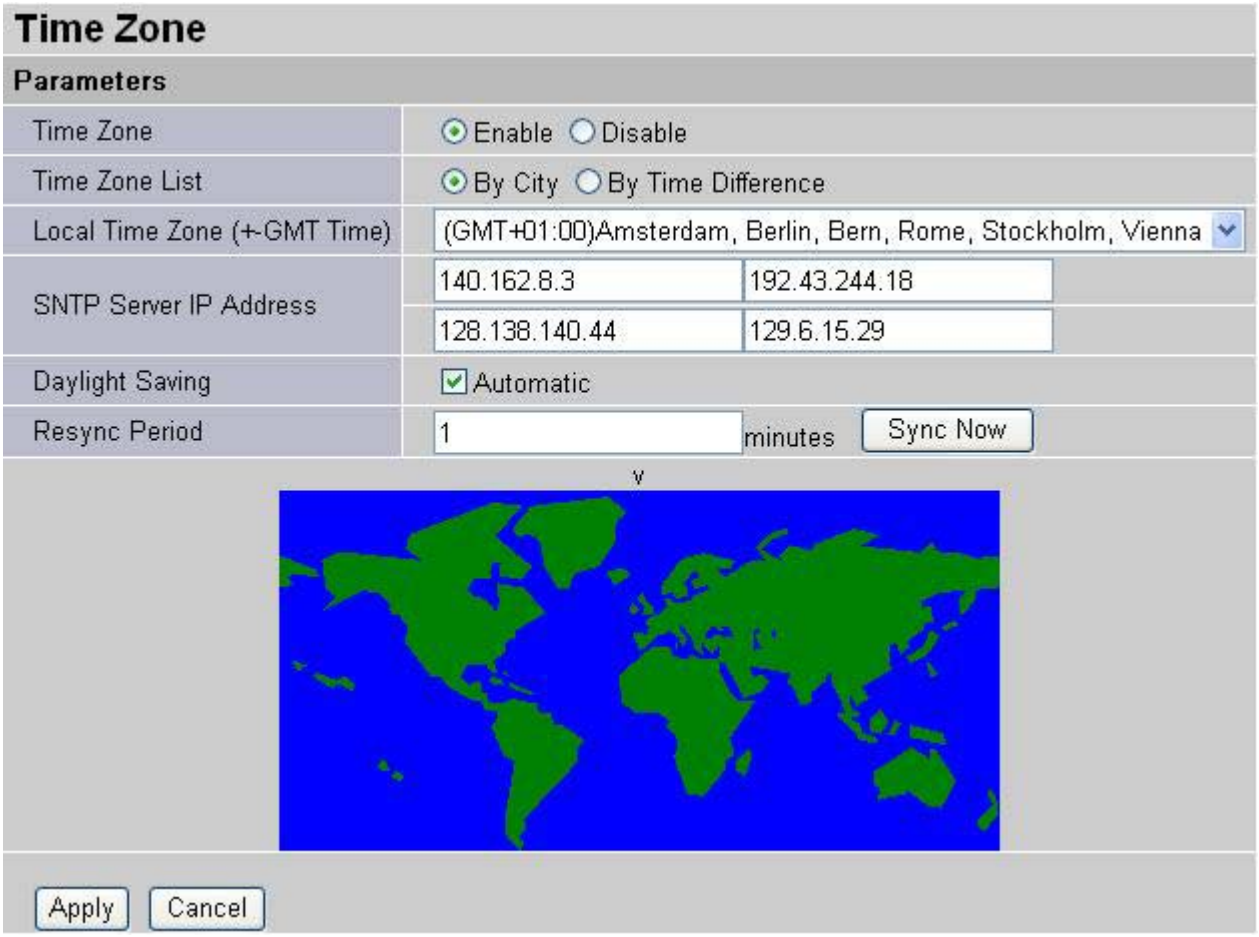
Connect Mode: The default is Multimode; it will detect the ADSL line code, G.dmt, G.lite, and T1.413 automatically. But in some area, it cannot detect the ADSL line code well. At this time, please adjust the ADSL line code to G.dmt or T1.413 first. If it still fails, please try the other values such as ALCTL, ADI, etc.
Activate Line: Aborting (false) your ADSL line and making it active (true) again for taking effect with setting of **Connect Mode**.
Tx Attenuation: Setting ADSL transmission gain, the value is between 0~12.
DSP FirmwareVersion: Current ADSL line code firmware version.
Connected: Display current ADSL line sync status.
Operational Mode: Display current ADSL mode standard (Operational Mode) your Router is using when ADSL line has sync.
Annex Type: ADSL Annex A, which works over a standard telephone line. Annex B, which works over an ISDN line.
Upstream: Display current upstream rate of your ADSL line.
Downstream: Display current downstream rate of your ADSL line.

3.6.3.3 System

There are six items under the SYSTEM section, Time Zone, Remote Access, Firmware Upgrade, Backup/Restore, Restart Router & User Management.

3.6.3.3.1 Time Zone

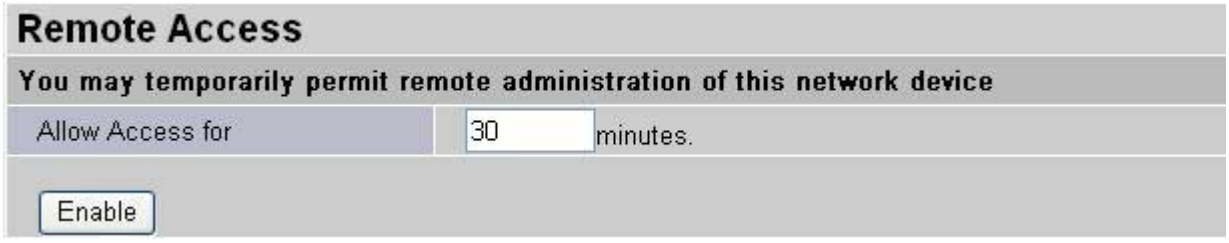
When you click **Time Zone**, you get the following figure.



The router does not have a real time clock on board; instead, it uses the simple network time protocol (SNTP) to get the current time from the SNTP server from the outside network. Please choose your local time zone, click **Enable**, **choose either By City or By Time Difference setting** and click the Apply button. You will get the correct time information after you really establish a connection to the Internet. If you prefer to enter your own SNTP server, please enter and use it as the first choice.

3.6.3.3.2 Remote Access

When you click **Remote Access** and then click **Enable**, you may temporarily permit remote administration of the ADSL Firewall Router.



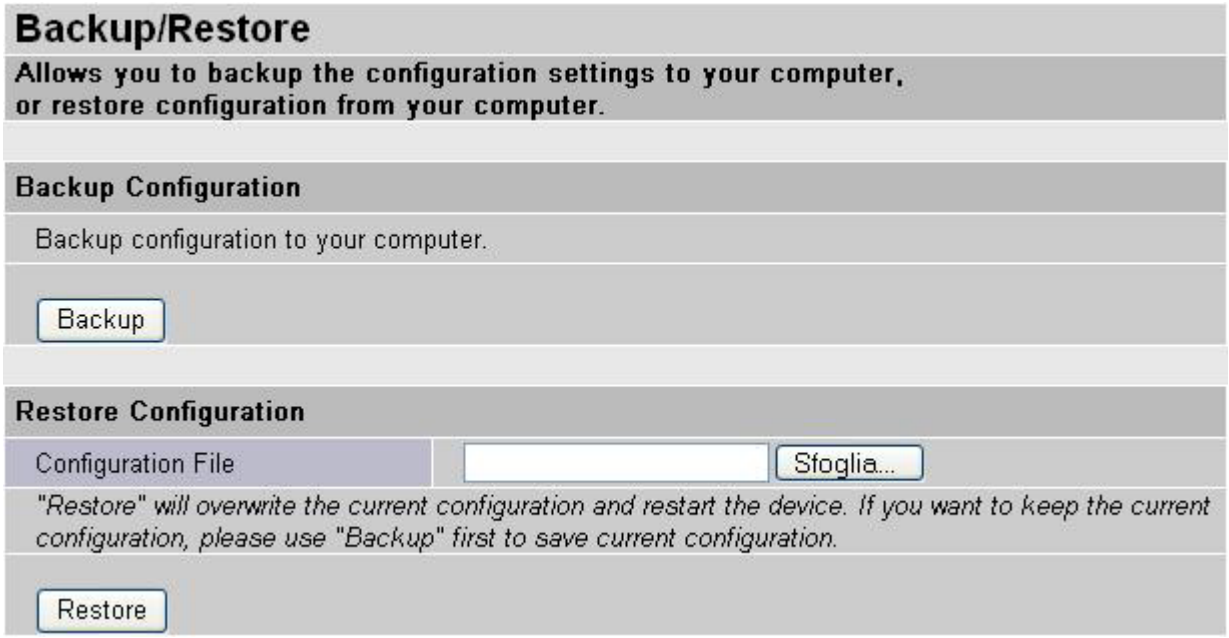
3.6.3.3.3 Firmware Upgrade

When you click **Firmware Upgrade**, it allows you to input the location of firmware stored on your PC and click the Upgrade button to upgrade to the new firmware.

Do NOT upgrade firmware on any Atlantis Land product over a wireless connection.
Failure of the device may result. Use only hard-wired network connections.

3.6.3.3.4 Backup / Restore

When you click **Backup/Restore,** it allows you to save your current settings into a file on your PC. If you like to restore it back (input the location of this configuration file in the PC and click the **Restore** button to save it back).


Backup/Restore
Allows you to backup the configuration settings to your computer,
or restore configuration from your computer.
Backup Configuration
Backup configuration to your computer.
Backup
Restore Configuration
Configuration File
Sfoglia...
"Restore" will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.
Restore

When you click **Restart Router**, you have two functions. One is to restart it with current settings and the other is to restart it with factory default settings if you check **Reset to factory default settings**.

When you click **User Management**, you are able to edit existing user's database or to create other user accessing this device.

3.6.3.4 Firewall

Your router includes a full SPI (Stateful Packet Inspection) firewall for controlling Internet access from your LAN, as well as helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation. Please see the **WAN** configuration section for more details on NAT) the router acts as a "natural" Internet firewall, as all PCs on your LAN will use private IP addresses that cannot be directly accessed from the Internet.

Firewall: Prevents access from outside your network. The router provides three levels of security support:

NAT natural firewall: This masks LAN users' IP addresses which are invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network.

This natural firewall is on when NAT function is enabled.

Firewall Security and Policy (General Settings): Inbound direction of Packet Filter rules to prevent unauthorized computers or applications accessing your local network from the Internet.

Intrusion Detection: Enable Intrusion Detection to detect, prevent and log malicious attacks.

Access Control: Prevents access from PCs on your local network:

Firewall Security and Policy (General Settings): Outbound direction of Packet Filter rules to prevent unauthorized computers or applications accessing the Internet.

MAC Filter rules: To prevent unauthorized computers accessing the Internet.

URL Filter: To block PCs on your local network from unwanted websites.

You can find six items under the Firewall section: General Settings, Packet Filter, Intrusion Detection, MAC Address Filter, URL Filter and Firewall Log.

You can choose not to enable Firewall, to add all filter rules by yourself, or enable the Firewall using preset filter rules and modify the port filter rules as required. The Packet Filter is divided into two sections: Port Filters and Address Filters, used to filter packets based-on Applications (Port) or IP addresses.

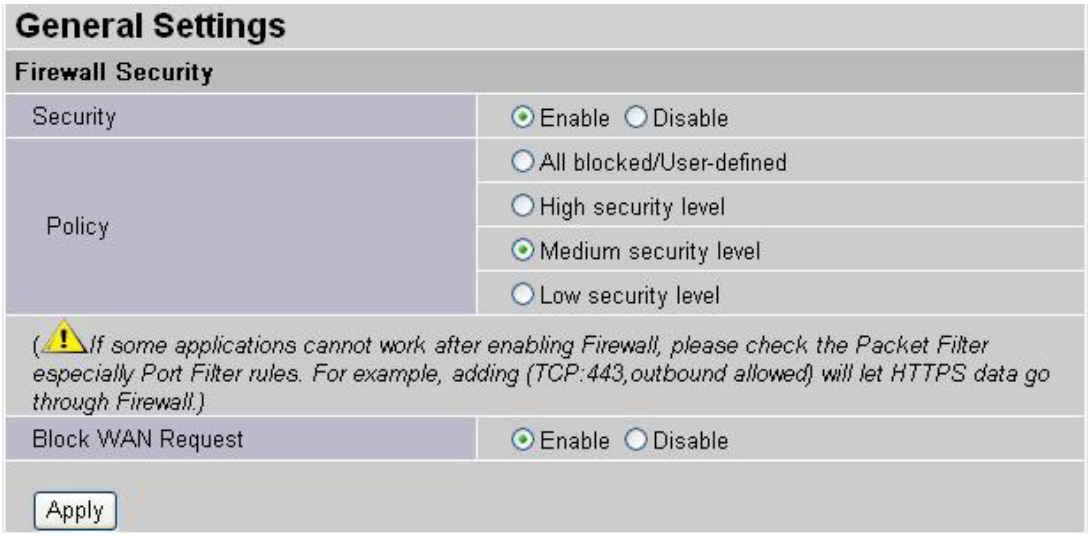
There are four options when you enable the Firewall, they are:

- All blocked/User-defined: no pre-defined port or address filter rules by default, meaning that all inbound (Internet to LAN) and outbound (LAN to Internet) packets will be blocked. Users have to add their own filter rules for further access to the Internet.
- High/Medium/Low security level: the pre-defined port filter rules for High, Medium and Low security are displayed in Port Filters of Packet Filter.

Select either **High, Medium** or **Low security level** to enable the Firewall. The only difference between these three security levels is the preset port filter rules in the Packet Filter. Firewall functionality is the same for all levels; it is only the list of preset port filter that changes between each setting.

If you choose of the preset security levels and then add custom filters, you may temporarily disable the firewall and recover your custom filter settings by re-selecting the same security level.

The "**Block WAN Request**" is a stand-alone function and not relate to whether security enable or disable. Mostly it is for preventing any scan tools from WAN site by hacker.



Firewall Security: When you enable Firewall function, you can select one of the firewall security policies.

All blocked/User-defined: By default, all of traffic between WAN and LAN are blocked. You have to configure the type of traffic passed between WAN and LAN, please refer to Packet Filter below.

High, Medium and Low security level: By default, your system uses High, Medium and Low firewall security level between the WAN and LAN. For example, when you select High, the Port Filters of Packet Filter screen will be set automatically according to High security level settings.

Look the table below for details:

Application	**Protocol**	**Port Number**		**Firewall (High)**		**Firewall(Medium)**		**Firewall (Low)**	
		Start	End	Inbound	Outbound	Inbound	Outbound	Inbound	Outbound
HTTP(80)	TCP(6)	80	80	NO	YES	NO	YES	NO	YES
DNS (53)	UDP(17)	53	53	NO	YES	NO	YES	NO	YES
DNS (53)	TCP(6)	53	53	NO	YES	NO	YES	NO	YES
FTP(21)	TCP(6)	21	21	NO	NO	NO	YES	NO	YES
Telnet(23)	TCP(6)	23	23	NO	NO	NO	YES	NO	YES
SMTP(25)	TCP(6)	25	25	NO	YES	NO	YES	NO	YES
POP3(110)	TCP(6)	110	110	NO	YES	NO	YES	NO	YES
NEWS(119)	TCP(6)	119	119	NO	NO	NO	YES	NO	YES
RealAudio (7070)	UDP(17)	7070	7070	NO	NO	YES	YES	YES	YES
ICMP	ICMP(1)	N/A	N/A	NO	YES	NO	YES	NO	YES
H.323(1720)	TCP(6)	1720	1720	NO	NO	NO	YES	YES	YES
T.120(1503)	TCP(6)	1503	1503	NO	NO	NO	YES	YES	YES
SSH(22)	TCP(6)	22	22	NO	NO	NO	YES	NO	YES
NTP(123)	UDP(17)	123	123	NO	YES	NO	YES	NO	YES
HTTPS(443)	TCP(6)	443	443	N/A	N/A	NO	YES	NO	YES
ICQ(5190)	TCP(6)	5190	5190	N/A	N/A	N/A	N/A	YES	YES
MSNP	TCP(6)	1863	1863	N/A	N/A	N/A	N/A	YES	YES
ASF3	UDP(17)	7001	7001	N/A	N/A	N/A	N/A	YES	YES
PPTP	TCP(1723)	1723	1723	N/A	N/A	N/A	N/A	N/A	N/A
IPSEC	UDP(6)	500	500	N/A	N/A	N/A	N/A	N/A	N/A

Firewall Logging: When both of Firewall Security and Firewall Logging are enabled, the device will detect the blocked and/or intrusion packets, once the setting has configured. Then the router will log the corresponding (blocking or intrusion detection) logs into the Event Log under Status.

The Firewall – Packet Filter is shown as below.

Packet Filter

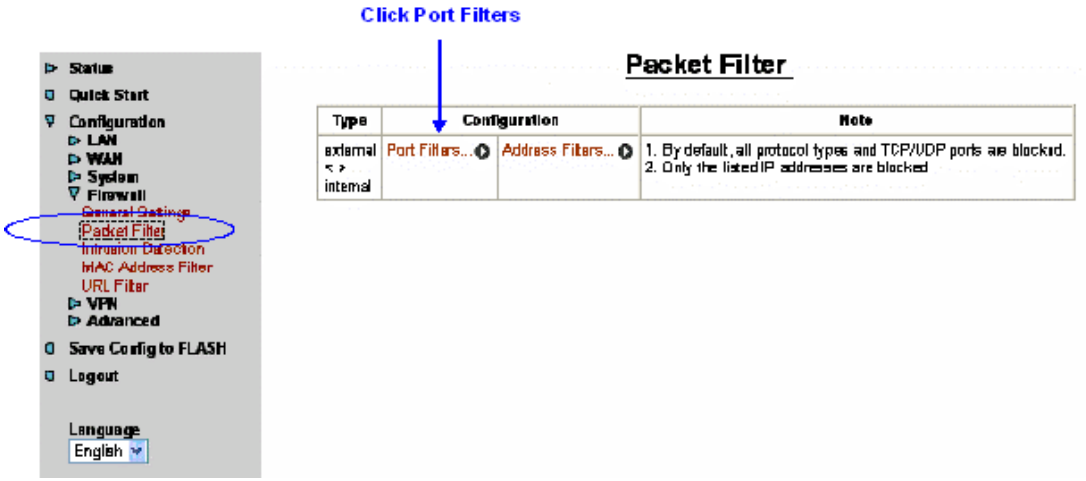
Firewall Security

Type	Configuration		Note
external < > internal	Port Filters	Address Filters	1. By default, all protocol types and TCP/UDP ports are blocked. 2. Only the listed IP addresses are blocked

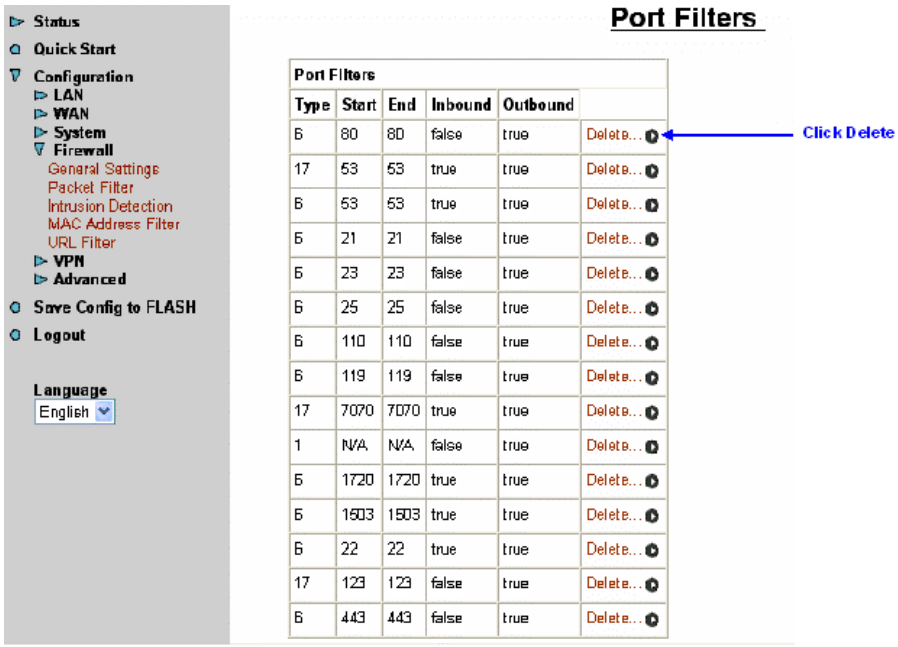
You may configure to filter inbound (incoming) and outbound (outgoing) packets based on PORT or IP address.
If it is based on PORT, click Port Filters for more options. You may filter the packets based on PORT and packet type (TCP or UDP or any). For example, the protocol number 1 means ICPM. You may enter 1 to protocol number of Raw IP Filtering web page. Port ranges are supported.
If it is based on IP address, click Address Filters for more options. You may enter the IP address and again to select the inbound or outbound packets.
For example, to allow TCP packet, port 0 to 1000 passing router between WAN and LAN and blocks host IP address, 192.168.1.100. Then you have to configure the port filter → add TCP filter > 0 to 1000 and ALLOW in both direction. Then click address filter → add address filter → enter host IP 192.168.1.100, subnet mask 255.255.255.0 and both direction.

3.6.3.4.1 Configuring Packet Filter

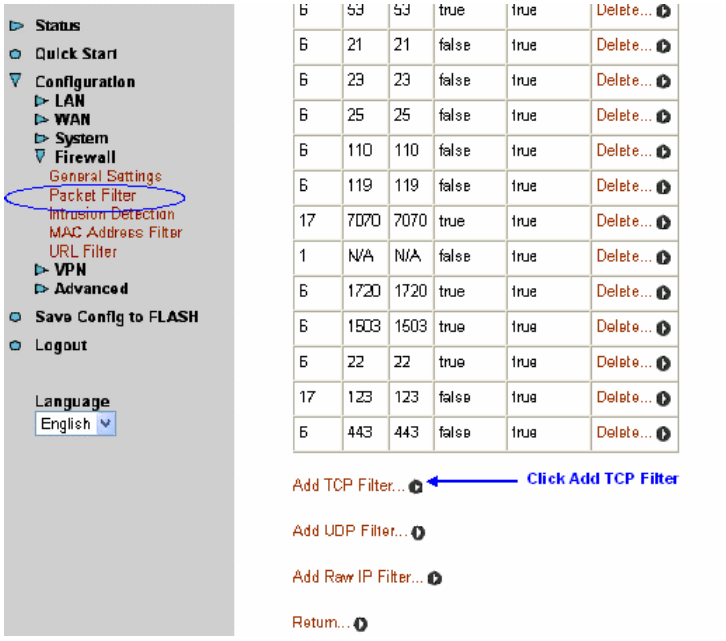
1. Click Packet Filter, you will get the following figure.



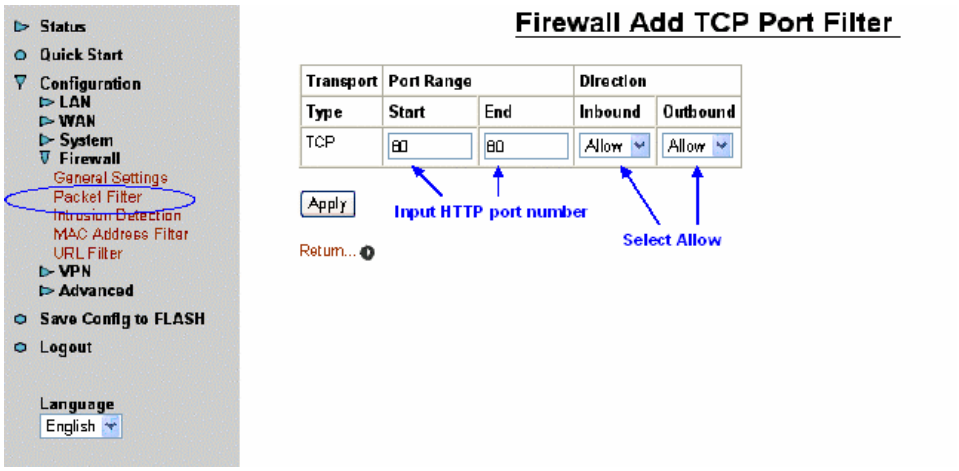
2. Click Port Filters, the pre-defined port filter rules screen of low security level is shown as below.



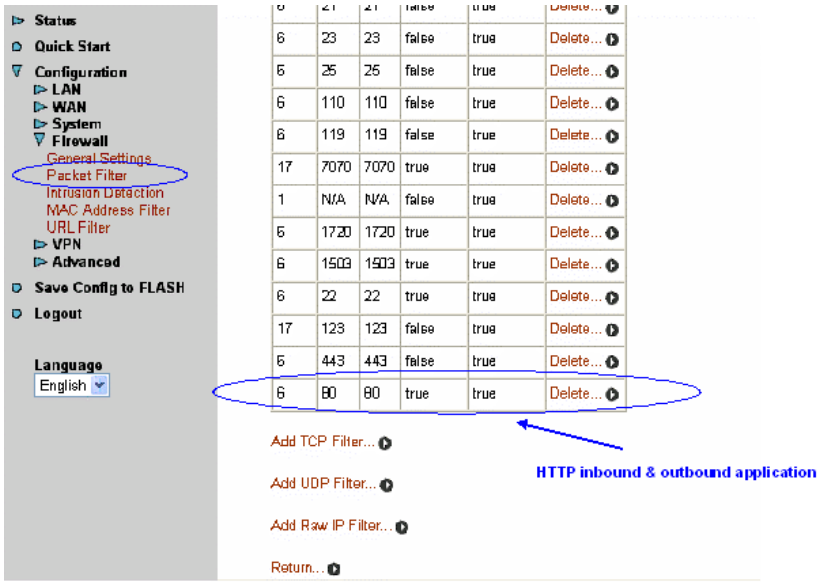
3. Click Delete to delete the HTTP rule.
4. Click Add TCP Filter.



5. Input the port number and set the inbound & outbound as Allow.



6. The port filter rule of HTTP is shown as below.



3.6.3.4.2 INTRUSION DETECTION

The router's *Intrusion Detection System* (IDS) is used to detect hacker attacks and intrusion attempts from the Internet. If the IDS function of the firewall is enabled, inbound packets are filtered and blocked depending on whether they are detected as possible hacker attacks, intrusion attempts or other connections that the router determines to be suspicious.

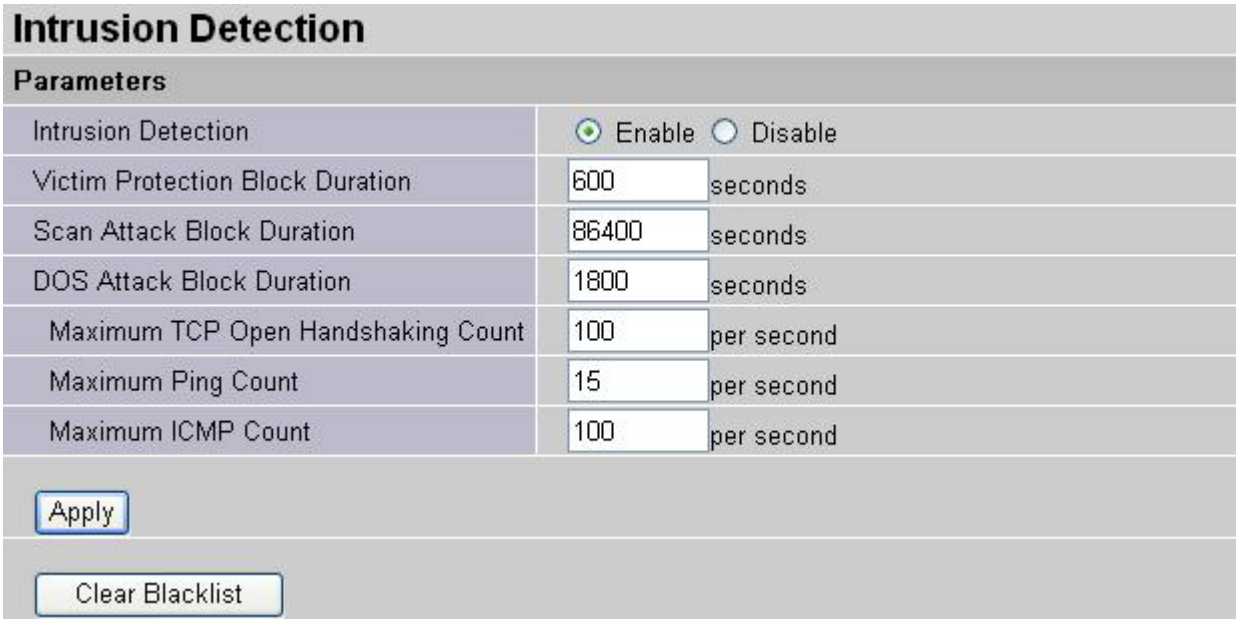
Blacklist: If the router detects a possible attack, the source IP or destination IP address will be added to the Blacklist. Any further attempts using this IP address will be blocked for the time period specified as the **Block Duration**. The default setting for this function is false (disabled). Some attack types are denied immediately without using the Blacklist function, such as *Land attack* and *Echo/CharGen scan*.

Block Duration:

- **DoS Attack Block Duration**: This is the duration for blocking hosts that attempt a possible Denial of Service (DoS) attack. Possible DoS attacks this attempts to block include *Ascend Kill* and *WinNuke*. Default value is 1800 seconds.

- **Scan Attack Block Duration**: This is the duration for blocking hosts that attempt a possible Scan attack. Scan attack types include *X'mas scan, IMAP SYN/FIN scan* and similar attempts. Default value is 86400 seconds.
- **Victim Protection Block Duration**: This is the duration for blocking *Smurf* attacks. Default value is 600 seconds.

Victim Protection: If enabled, IDS will block Smurf attack attempts. Default is false.
Max TCP Open Handshaking Count: This is a threshold value to decide whether a *SYN Flood* attempt is occurring or not. Default value is 100 TCP SYN per seconds.
Max PING Count: This is a threshold value to decide whether an *ICMP Echo Storm* is occurring or not. Default value is 15 ICMP Echo Requests (PING) per second.
Max ICMP Count: This is a threshold to decide whether an *ICMP flood* is occurring or not. Default value is 100 ICMP packets per seconds except ICMP Echo Requests (PING).
For *SYN Flood*, *ICMP Echo Storm* and *ICMP flood*, IDS will just warn the user in the Event Log. It cannot protect against such attacks.

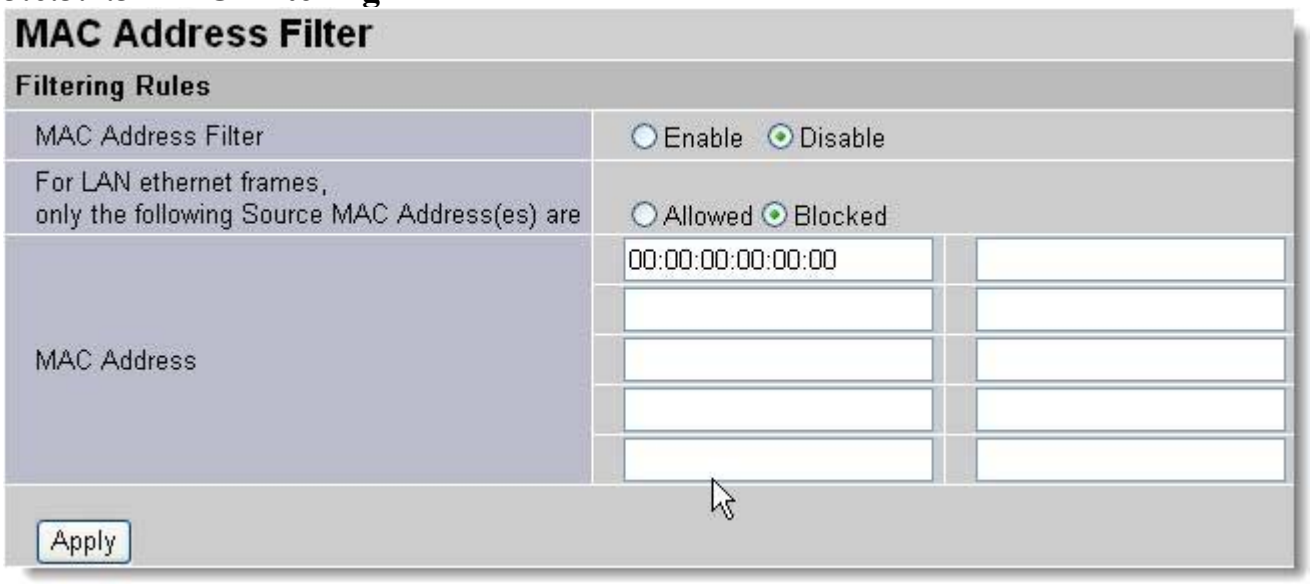


Hacker attack types recognized by the IDS

Attack	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
Ascend Kill	Ascend Kill	Src IP	DoS	Yes	Yes
Win Nuke	TCP, Port=135, 137-139 Flag:URG	Src IP	DoS	Yes	Yes
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
Land Attack	SrcIP = DstIP			Yes	Yes
Echo/CharGen Scan	UDP Echo Port and CharGen Port			Yes	Yes
Echo Scan	UDP Dst Port =Echo(7)	Src IP	Scan	Yes	Yes
CharGen Scan	UDP Dst Port =CharGen(19)	Src IP	Scan	Yes	Yes
X'Mas Tree Scan	TCP Flag: X'mas	Src IP	Scan	Yes	Yes
IMAP SYN/FIN Scan	TCP Flag: SYN/FIN DstPort: IMAP(143)	Src IP	Scan	Yes	Yes

	SrcPort: 0 or 65535				
SYN/FIN/RST/ACK Scan	TCP, No Existing session And Scan Hosts more than five	Src IP	Scan	Yes	Yes
Net Bus Scan	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	Src IP	Scan	Yes	Yes
Back Orifice Scan	UDP, DstPort=Orifice Port (31337)	Src IP	Scan	Yes	Yes
SYN Flood	Max TCP Open Handshaking Count(Def=100 s)				Yes
ICMP Flood	Max ICMP Count (Def=100 s)				Yes
ICMP Echo	Max Ping Count (Def=15 s)				Yes

3.6.3.4.3 MAC Filtering

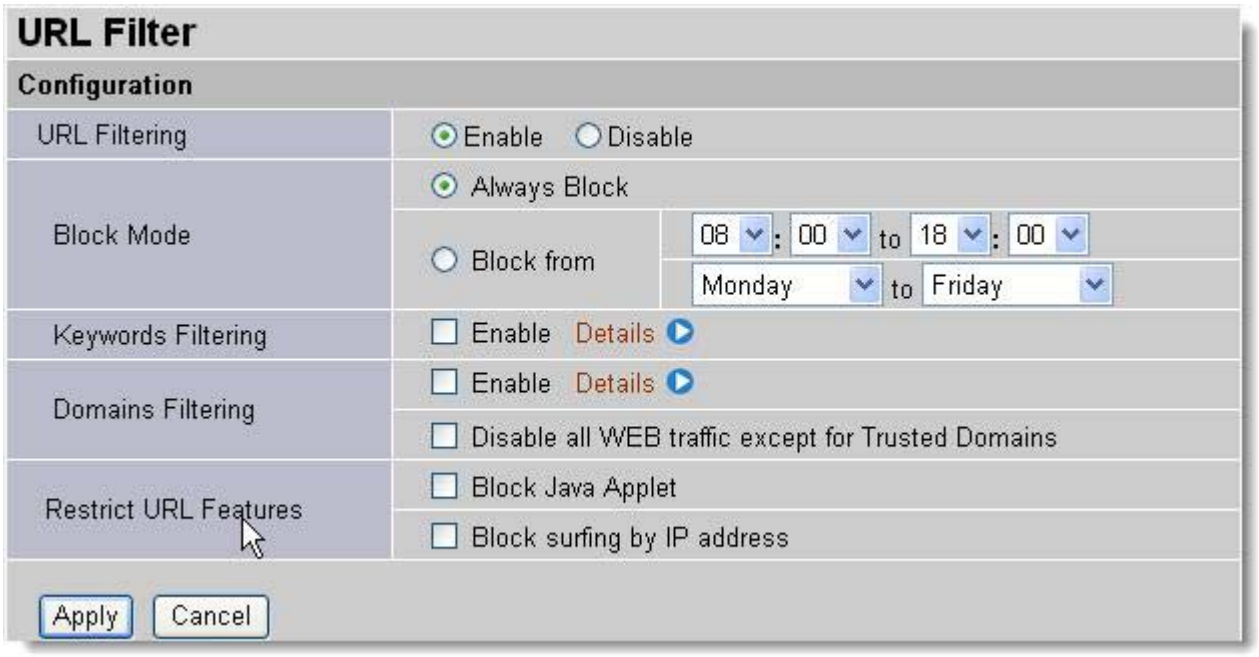


MAC filtering function enables you to configure your ADSL Firewall Router to block internal user (**MAC address**) from Internet access.

⊙ **Enable / Disable:** Check **Enable / Disable** radio button to active / disable, in respectively, the MAC address filter function. If you check **Enable,** remember to choose either **Allowed** or **Blocked** the MAC Address listed in the table, as shown above. If you select **Blocked**, the packet with the MAC address in the table will be dropped and others will be forwarded. If you select **Allowed**, the packet with the MAC address in the table will be forwarded and others will be dropped. Then select **Apply** button to save the setting.

3.6.3.4.4 URL Filtering

URL filter rules allow you to prevent users on your network from accessing particular websites by their URL. There are no predefined URL filter rules; you can add filter rules to meet your requirements.



Keywords Filtering:

Allows blocking by specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called "advertisement.gif").

When enabled, your specified keywords list will be checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked.

Please note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

For example, if the URL is http://www.helloworld.com.tw/abcde.html, it will be dropped as the keyword "abcde" occurs in the URL.

Domains Filtering:

This function checks the domain name in URLs accessed against your list of domains to block or allow. If it is matched, the URL request will be sent (Trusted) or dropped (Forbidden). The checking procedure is:

1. Check the domain in the URL to determine if it is in the trusted list. If yes, the connection attempt is sent to the remote web server.
2. If not, check if it is listed in the forbidden list, and if present then the connection attempt is dropped..
3. If the packet does not match either of the above two items, it is sent to the remote web server.
4. Please be note that the domain only should be specified, not the full URL. For example to block traffic to www.sex.com, enter "sex" or "sex.com" instead of "www.sex.com". In the example below, the URL request for www.helloworld.com.tw will be sent to the remote web server because it is listed in the trusted list, whilst the URL request for www.sex or www.sex.com will be dropped, because helloworld.com is in the forbidden list.

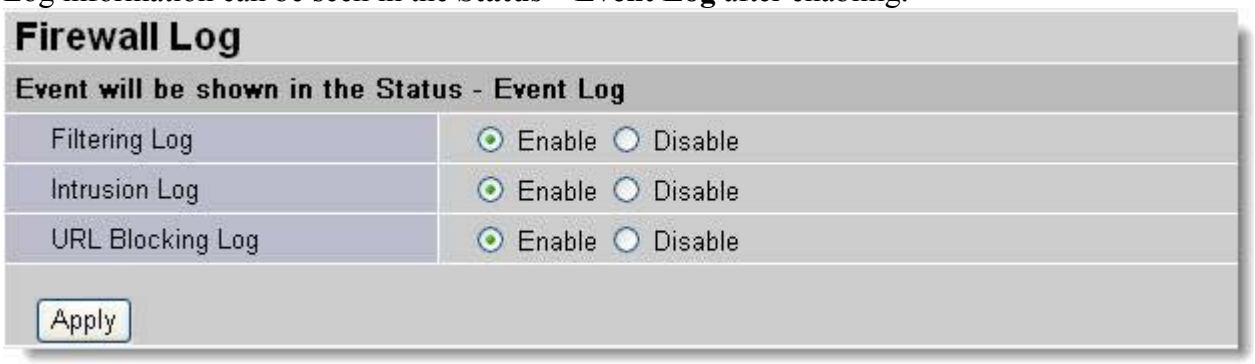
Restrict URL Features:

Block Java Applet: This function can block Web content which including the Java Applet. It is for preventing someone who wants to damage your system via standard HTTP protocol.

Block surfing by IP address: Preventing someone who uses the IP address as URL for skipping **Domains Filtering** function.

3.6.3.4.5 Firewall Log

Firewall Log display log information of any unexpected action with your firewall settings.
Check the **Enable** box to activate the logs.
Log information can be seen in the **Status – Event Log** after enabling.

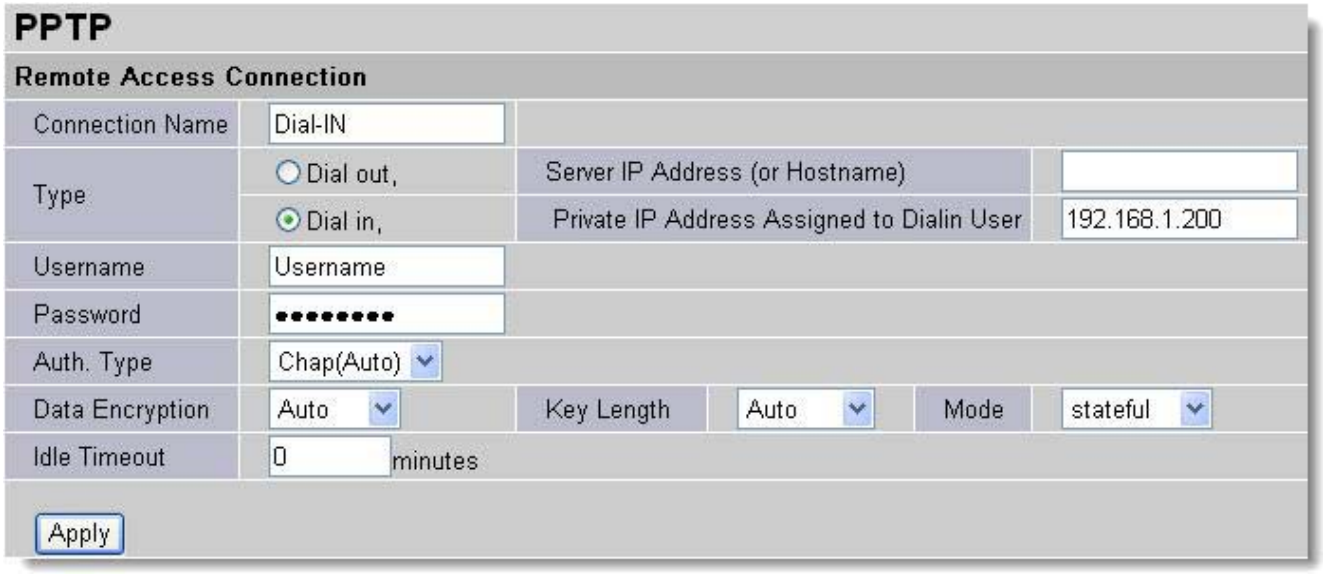


3.6.3.5 VPN

Your router support 2 main types of VPN (Virtual Private Network), PPTP and IPSec, and these are the two major section choices from the menu on the left. Click **Create** to select one of applications to continually setup.

VPN - PPTP

The router supports PPTP VPN to establish secure, end-to-end private network connections over a public networking infrastructure. There are two kinds of PPTP VPN connections, one is remote access (dial-in & dial-out), and the other is LAN-to-LAN access.
Deploying a remote access VPN enables users to reduce the cost by leveraging the local dial-up infrastructures of the ISP, in addition, transmitting data over a secure VPN tunnel.
LAN-to-LAN PPTP VPN is an alternative WAN infrastructure that is used to connect offices and home offices to share network resources with each other over a secure VPN tunnel.
There are two types of PPTP VPN supported, Remote Access and LAN-to-LAN (please refer below for more information.). Click Create to configure a new VPN connection.



Connection Name: This allows you to identify this particular connection, e.g. "Connection to office LAN".
Type: Check **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), check **Dial In** operates as a VPN server.

- When configuring your router as a Client, enter the remote **Server IP Address (or Hostname)** you wish to connection to.
- When configuring your router as a server, enter the **Private IP Address Assigned to Dial in User** address.

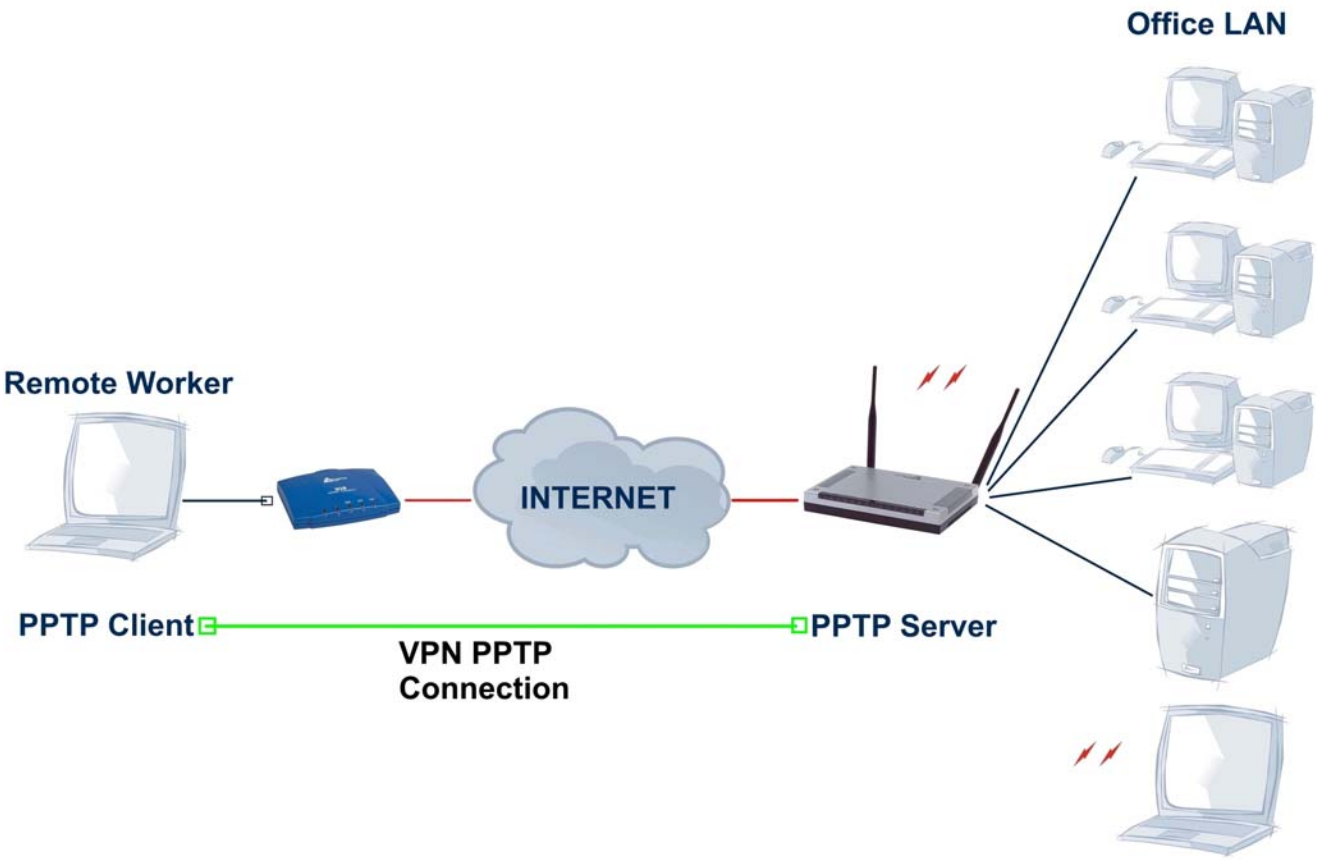
Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.
Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.
PPP Authentication Type: Default is **Auto** if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password

before sending, and also allows for challenges at different periods to ensure that the client has not been replaced by an intruder.
Data Encryption: Data sent over the VPN connection can be encrypted by an MPPE algorithm. Default is **Auto,** so that this setting is negotiated when establishing a connection, or else you can manually **Enable** or **Disable** encryption.
Key Length: The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is **Auto**, it is negotiated when establishing a connection. 128 bit keys provide stronger encryption than 40 bit keys.
Mode: You may select **Stateful** or **Stateless** mode. The key will be changed every 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.
Idle Time: Auto-disconnect the VPN connection when there is no activity on the connection for a predetermined period of time. 0 means this connection is always on.
Click **Apply** after changing settings.

An Example of Configuring a Remote Access PPTP VPN Dial-in Connection

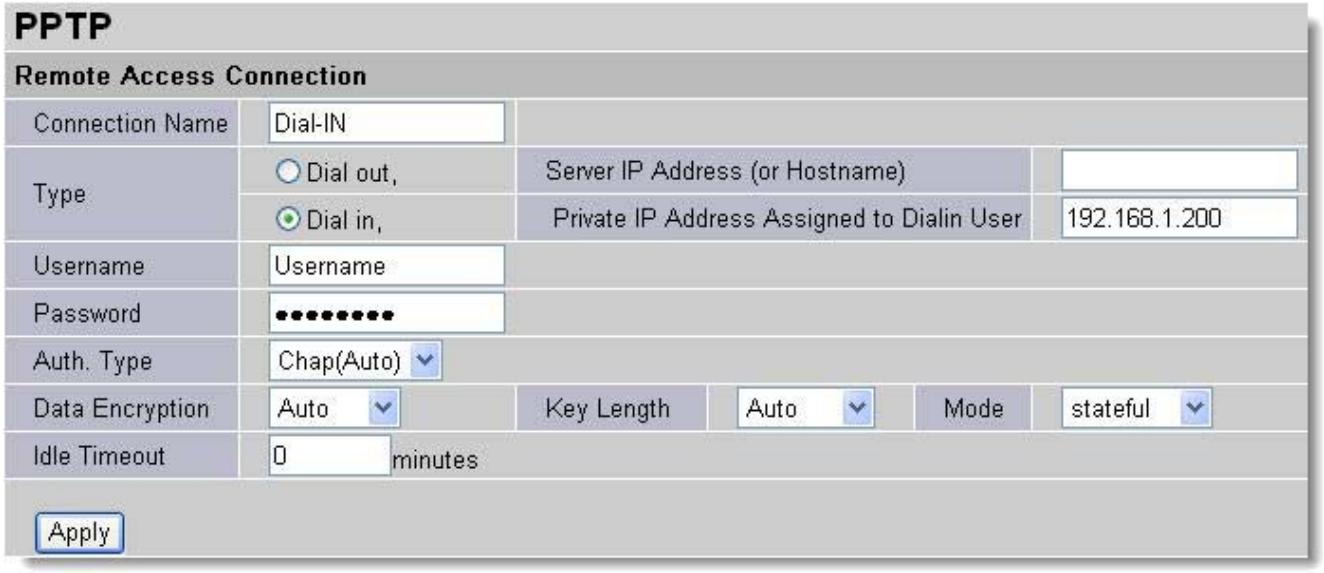
Background of the Example
A remote worker establishes a PPTP VPN connection with the head office using Microsoft's VPN Adapter, a piece of software included with Windows 2000/ME, etc. The Router is installed in the Office Lan, connected to a couple of PCs and Servers.

Application Diagram



Configuring PPTP VPN in the Office LAN Router

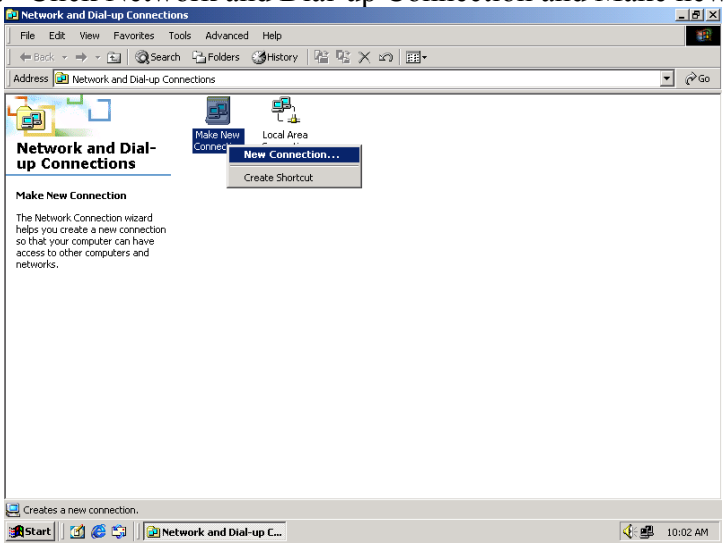
The input IP address 192.168.1.200 will be assigned to the remote worker, please make sure this IP is not used in the Office LAN.



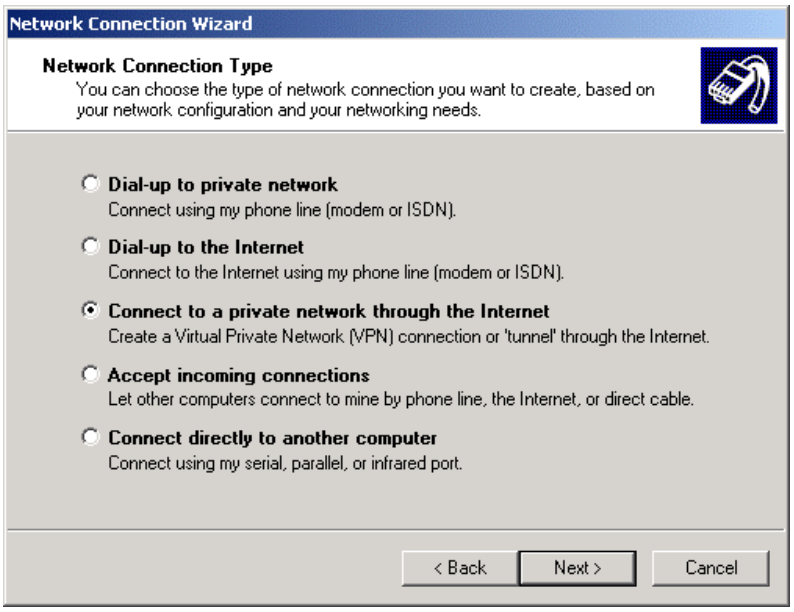
Configuring PPTP VPN in Remote Side

You can configure VPN client with commercial VPN client software package (e.g. SSH) or the Dial-up Adaptor in Windows. Please follow the steps below if you are a Windows 2000/XP user.

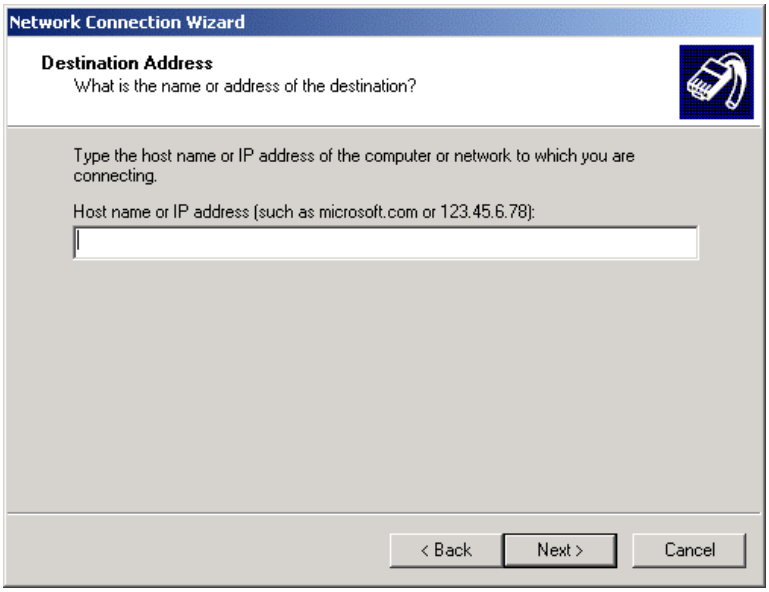
1. Click Network and Dial-up Connection and Make new connection


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Address Network and Dial-up Connections
Network and Dial-up Connections
Make New Connection
The Network Connection wizard helps you create a new connection so that your computer can have access to other computers and networks.
Make New Connec...
Local Area
New Connection...
Create Shortcut
Creates a new connection.
Start
Network and Dial-up C...
10:02 AM

2. Follow the step and select "**Connect to a private network through the Internet**"


Network Connection Wizard
Network Connection Type
You can choose the type of network connection you want to create, based on your network configuration and your networking needs.
Dial-up to private network
Connect using my phone line (modem or ISDN).
Dial-up to the Internet
Connect to the Internet using my phone line (modem or ISDN).
Connect to a private network through the Internet
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.
Accept incoming connections
Let other computers connect to mine by phone line, the Internet, or direct cable.
Connect directly to another computer
Connect using my serial, parallel, or infrared port.
< Back
Next >
Cancel

3. Enter the IP address of the ADSL Router located in the office Lan (or Dynamic DNS name).


Network Connection Wizard
Destination Address
What is the name or address of the destination?
Type the host name or IP address of the computer or network to which you are connecting.
Host name or IP address (such as microsoft.com or 123.45.6.78):
< Back
Next >
Cancel

4. Follow the step, the following screen appears. The setup is completed.

Network Connection Wizard
Completing the Network Connection Wizard
Type the name you want to use for this connection:
Virtual Private Connection
To create this connection and save it in the Network and Dial-up Connections folder, click Finish.
To edit this connection in the Network and Dial-up Connections folder, select it, click File, and then click Properties.
Add a shortcut to my desktop
< Back
Finish
Cancel

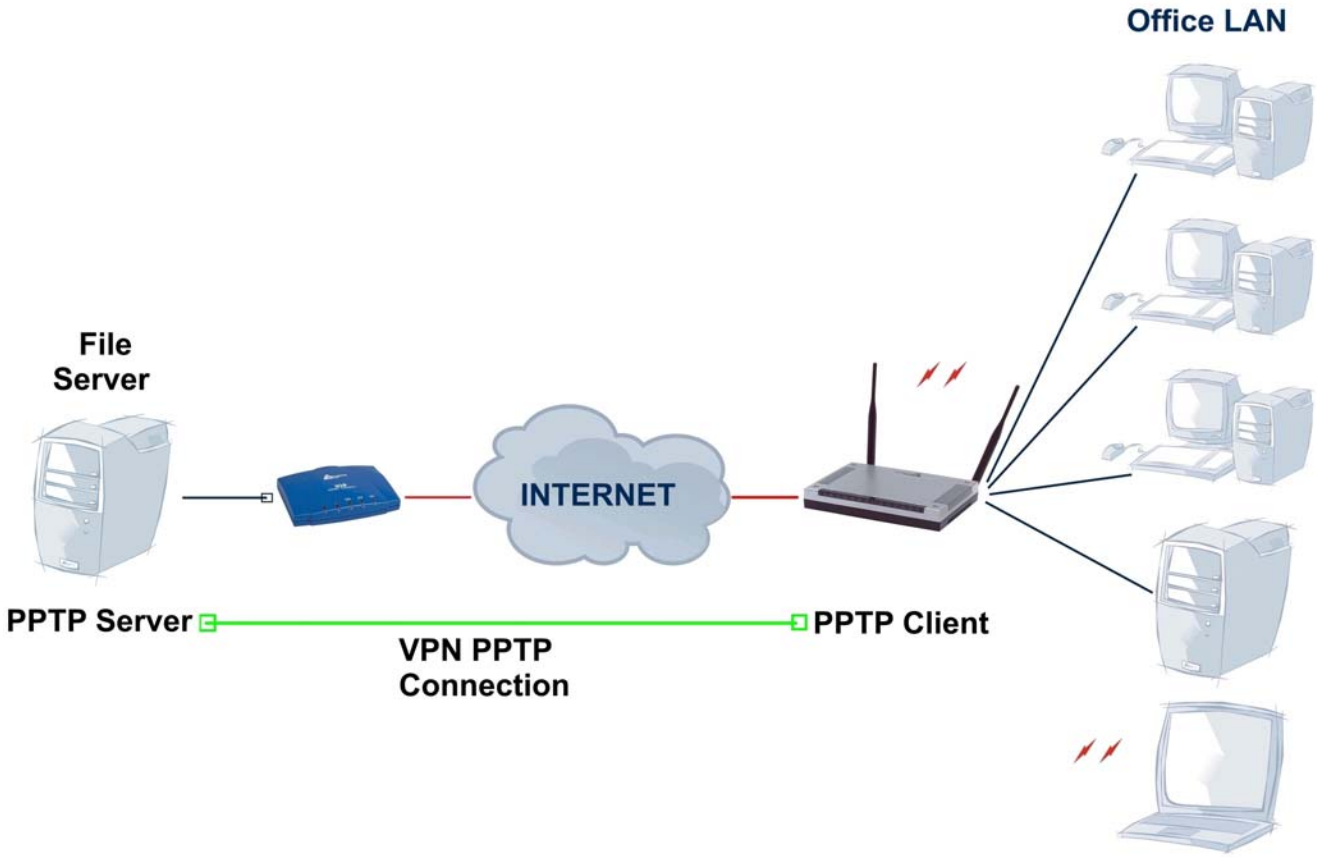
5. To make the connection, click the Virtual Private Connection icon in Dial-up Networking Group, and input the username & password set in ADSL Router.

An Example of Configuring a Remote Access PPTP VPN Dial-out Connection

Background of the Example

Corporate establishes a PPTP VPN connection with the file server located in the remote side. The router is installed in the office, connected with a couple of PCs and Servers.

Application Diagram



Configuring PPTP VPN in the Office

You can either input the IP address (80.123.23.45 in this case) or hostname to reach the Server.

PPTP

Remote Access Connection

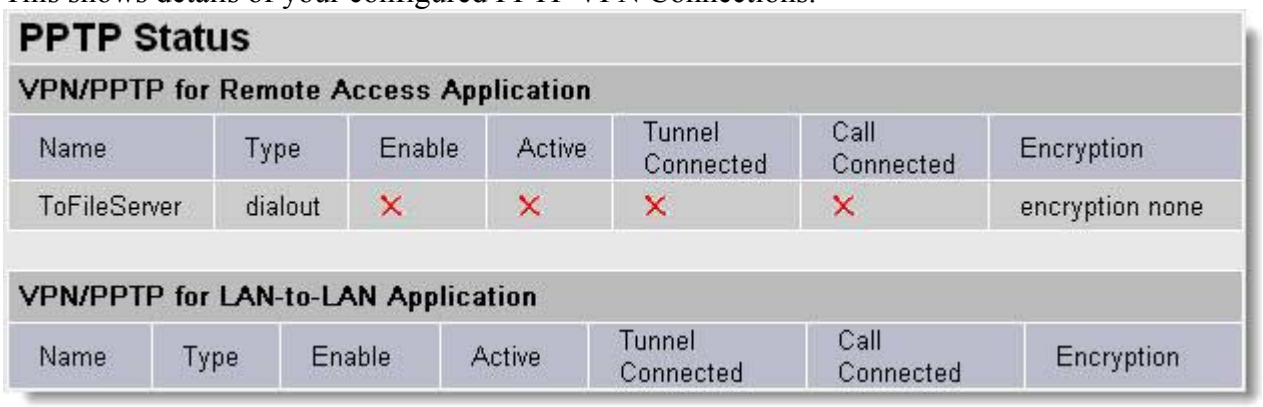
Connection Name	ToFileServer		
Type	Dial out,	Server IP Address (or Hostname)	80.123.23.45
	Dial in,	Private IP Address Assigned to Dialin User	
Username	username		
Password	••••••••		
Auth. Type	Chap(Auto)		
Data Encryption	Auto	Key Length: Auto	Mode: stateful
Idle Timeout	0 minutes		

Apply

Refer also to **PPTP VPN – remote access (dial-in)** for the other parameters.

PPTP Status

This shows details of your configured PPTP VPN Connections.



PPTP Status

VPN/PPTP for Remote Access Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption
ToFileServer	dialout	✕	✕	✕	✕	encryption none

VPN/PPTP for LAN-to-LAN Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

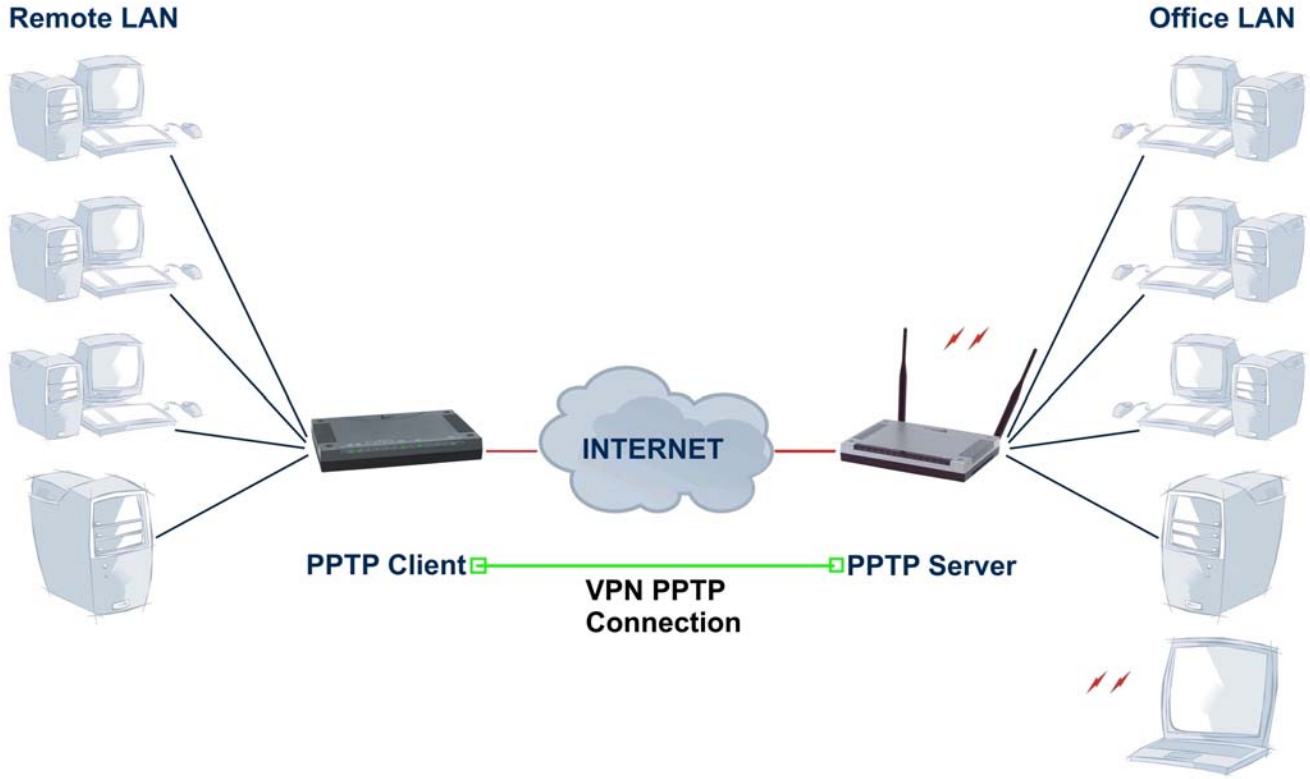
Name: The name you assigned to the particular PPTP connection in your VPN configuration.
Type: The type of connection (dial-in/dial-out).
Enable: Whether the connection is currently enabled.
Active: Whether the connection is currently active.
Tunnel Connected: Whether the VPN Tunnel is currently connected.
Call Connected: If the Call for this VPN entry is currently connected.
Encryption: The encryption type used for this VPN connection.

An Example of Configuring a LAN-to-LAN PPTP VPN Connection

Background of the Example

The Remote LAN establishes a PPTP VPN tunnel with the Office LAN to connect two private networks by leveraging the Internet infrastructure. The routers are installed in the Office Lan and Remote Lan accordingly.

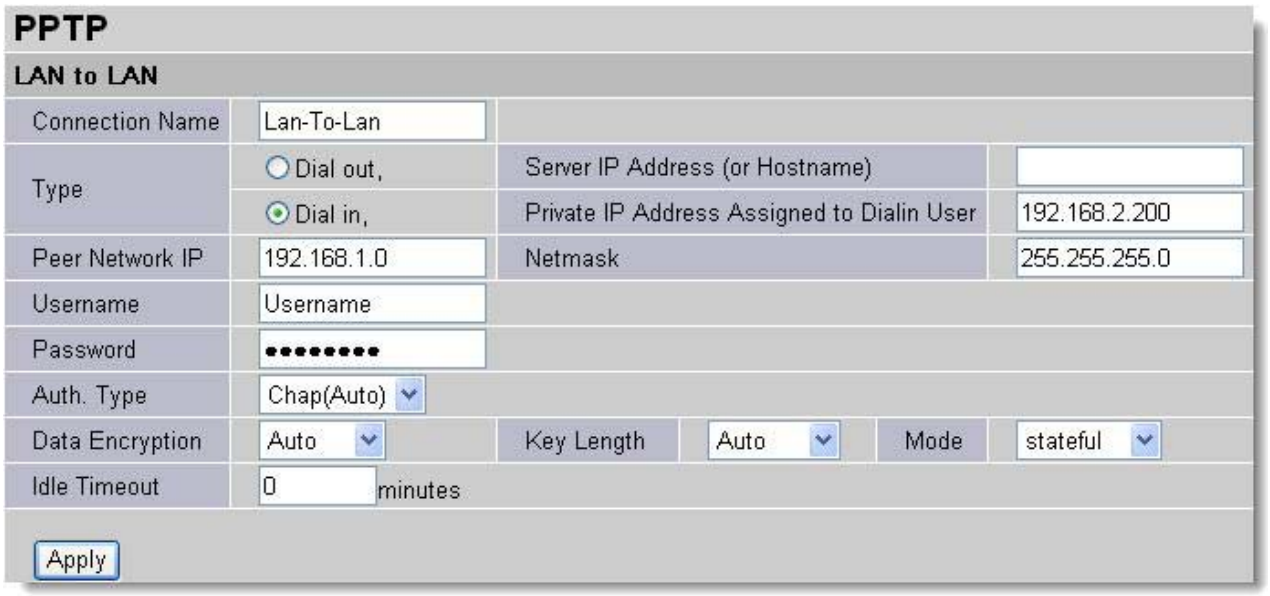
Application Diagram



	Remote LAN	Office LAN
Product Code	A02-RA3+	A02-WRA4-54G
Picture		
Public IP	80.17.56.78	69.121.1.32
NAT	Yes	Yes
LAN IP	192.168.1.X	192.168.2.X
Subnet Mask	255.255.255.0	255.255.255.0
PPTP	Client PPTP	Server PPTP

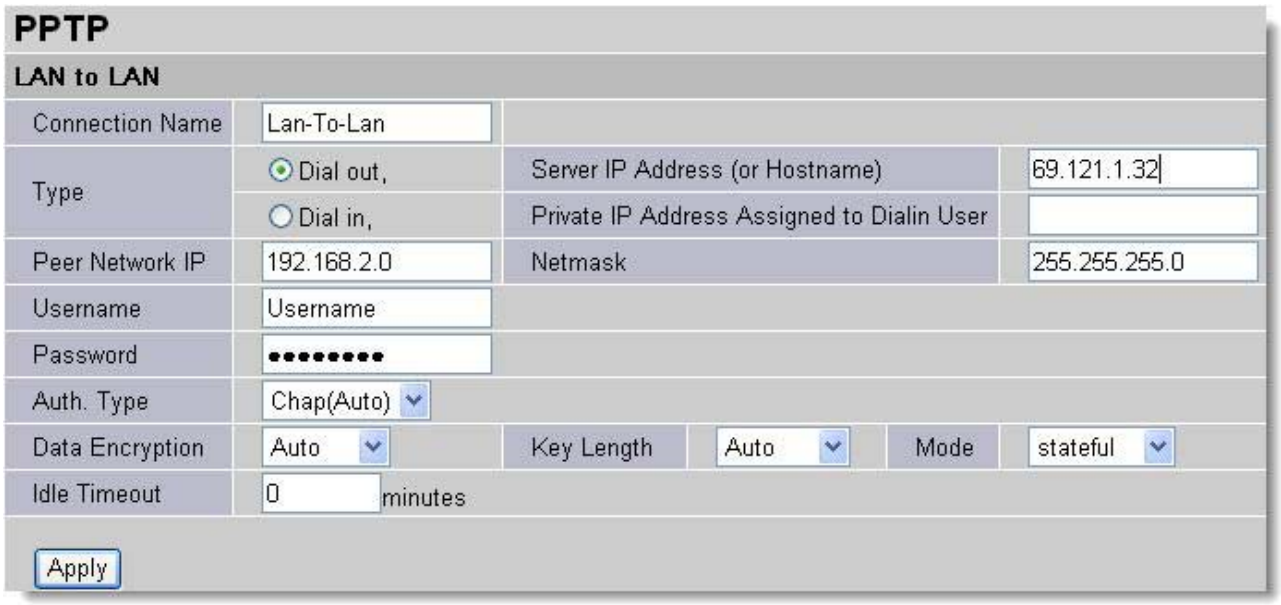
Configuring PPTP VPN in the Office Lan

The input IP address 192.168.2.200 will be assigned to the router located in the Remote LAN. Please make sure this IP is not used in the head office LAN.



Configuring PPTP VPN in the Remote Lan

The input IP address 69.121.1.32 is the **Public IP** address of the router located in the Office Lan. If you have a domain name assigned to this IP address - either you registered the DDNS (please refer to the **DDNS** section), or you have a static IP with a domain name, you can also use the Hostname instead of the IP address to reach the router.

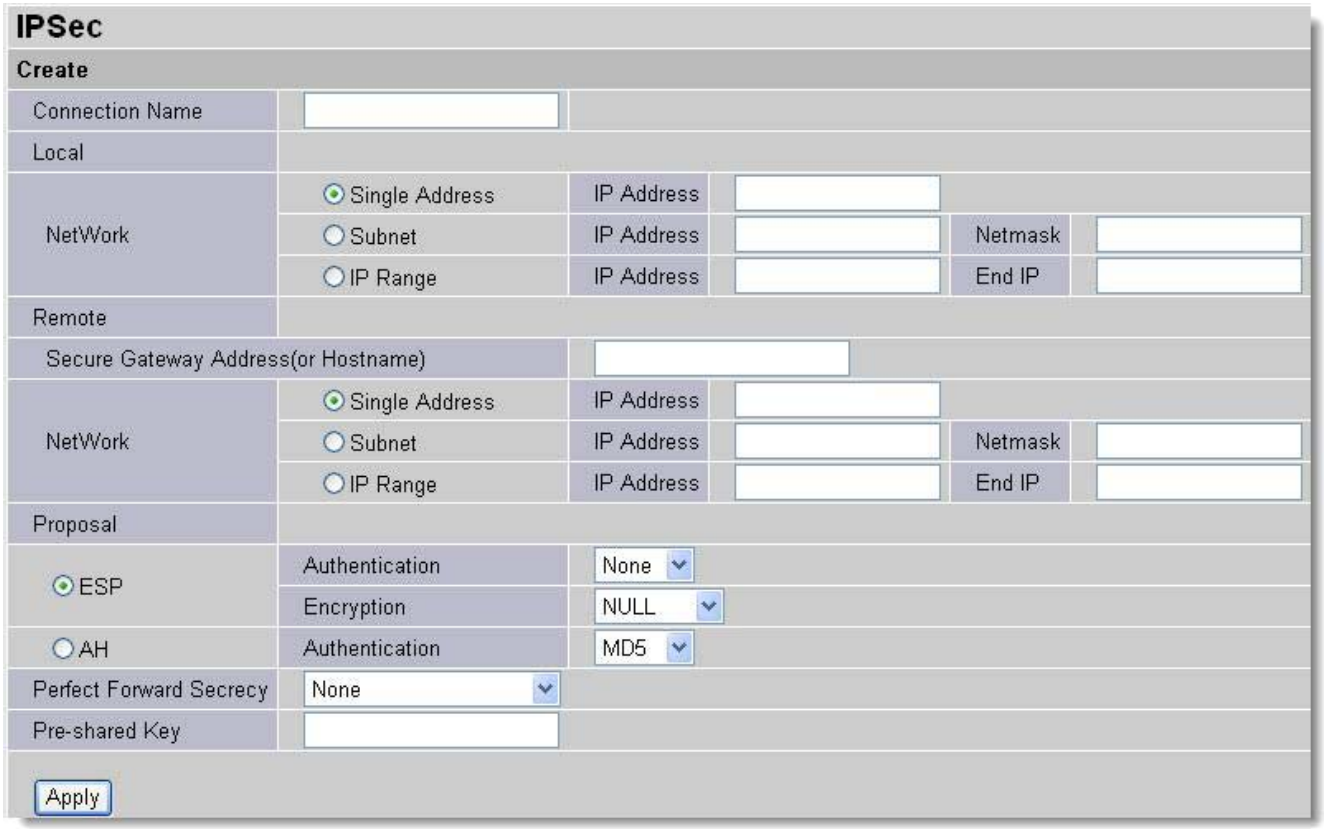


Refer also to **Configuring PPTP VPN in the Office LAN** for other parameters.

PPTP Status in the Office LAN
This shows details of your configured PPTP VPN Connections.
Name: The name you assigned to the particular PPTP connection in your VPN configuration.
Type: The type of connection (dial-in/dial-out).
Enable: Whether the connection is currently enabled.
Active: Whether the connection is currently active.
Tunnel Connected: Whether the VPN Tunnel is currently connected.
Call Connected: If the Call for this VPN entry is currently connected.
Encryption: The encryption type used for this VPN connection.

VPN - IPSec

The router supports IPSec VPN to establish secure, end-to-end private network connections over a public networking infrastructure.



Connection Name: A user-defined name for the connection (e.g. "To Remote Lan or To Office LAN ").

Local:

Local Network: Set the IP address, subnet or address range of the local network.

- **Single Address:** The IP address of the local host.
- **Subnet:** The subnet of the local network. For example, IP: 192.168.1.0 with netmask 255.255.255.0 specifies one class C subnet starting from 192.168.1.1 (i.e. 192.168.1.1 through to 192.168.1.254).
- **IP Range:** The IP address range of the local network. For example, IP: 192.168.1.1, end IP: 192.168.1.10

Remote:

- **Secure Gateway Address (or hostname):** The IP address or hostname of the remote VPN device that is connected and establishes a VPN tunnel.
- **Network:** Set the IP address, subnet or address range of the remote network.

Proposal:

- **Proposal:** Select the IPSec security method. There are two methods of checking the authentication information, AH (authentication header) and ESP (Encapsulating Security Payload). Use ESP for greater security so that data will be encrypted and authenticated.
  Using AH data will be authenticated but not encrypted.
- **Authentication:** Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA-1**) or **NONE**. SHA-1 is more resistant to brute-force attacks than MD5, however it is slower.

- **MD5:** A one-way hashing algorithm that produces a 128-bit hash.
- **SHA-1:** A one-way hashing algorithm that produces a 160-bit hash.

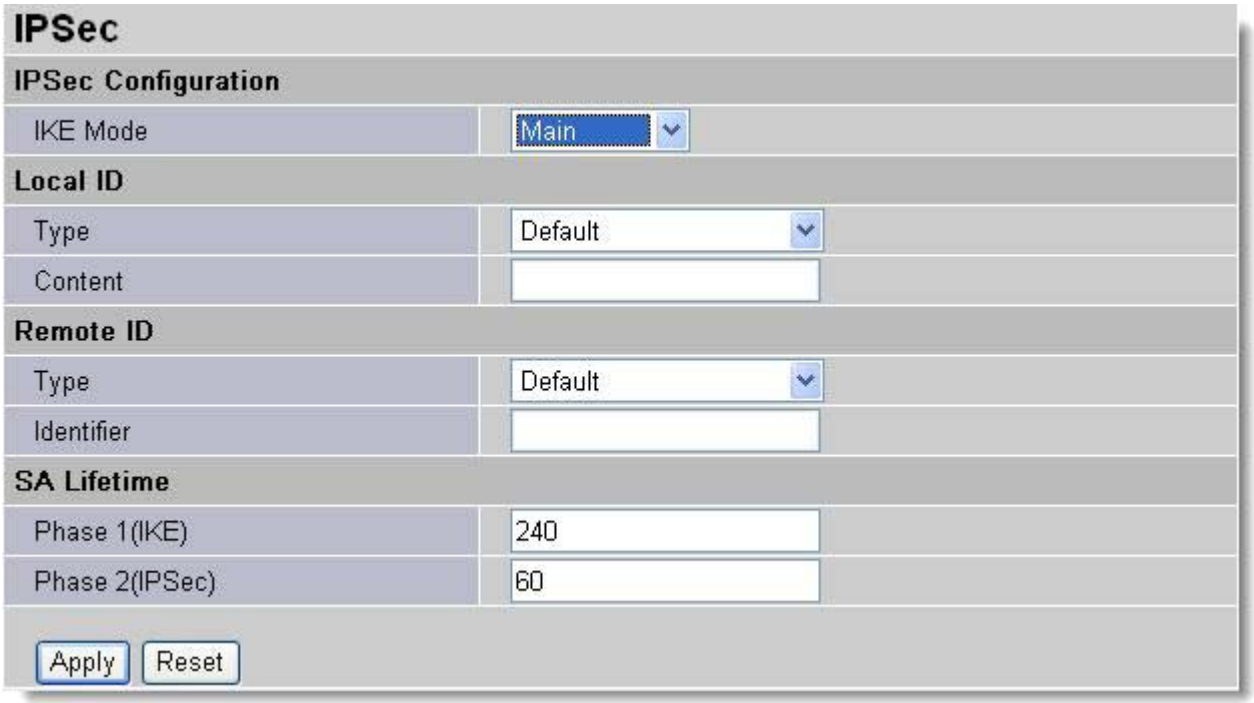
- **Encryption:** Select the encryption method from the pull-down menu. There are four options, DES, 3DES, AES and NONE. NONE means it is a tunnel only with no encryption. 3DES and AES are more powerful but increase latency.
  - **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
  - **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
  - **AES:** Stands for Advanced Encryption Standards, it uses 128 bits as an encryption method.

Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman publickey cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie- Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key.
Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Select the **Save** button to save the setting.

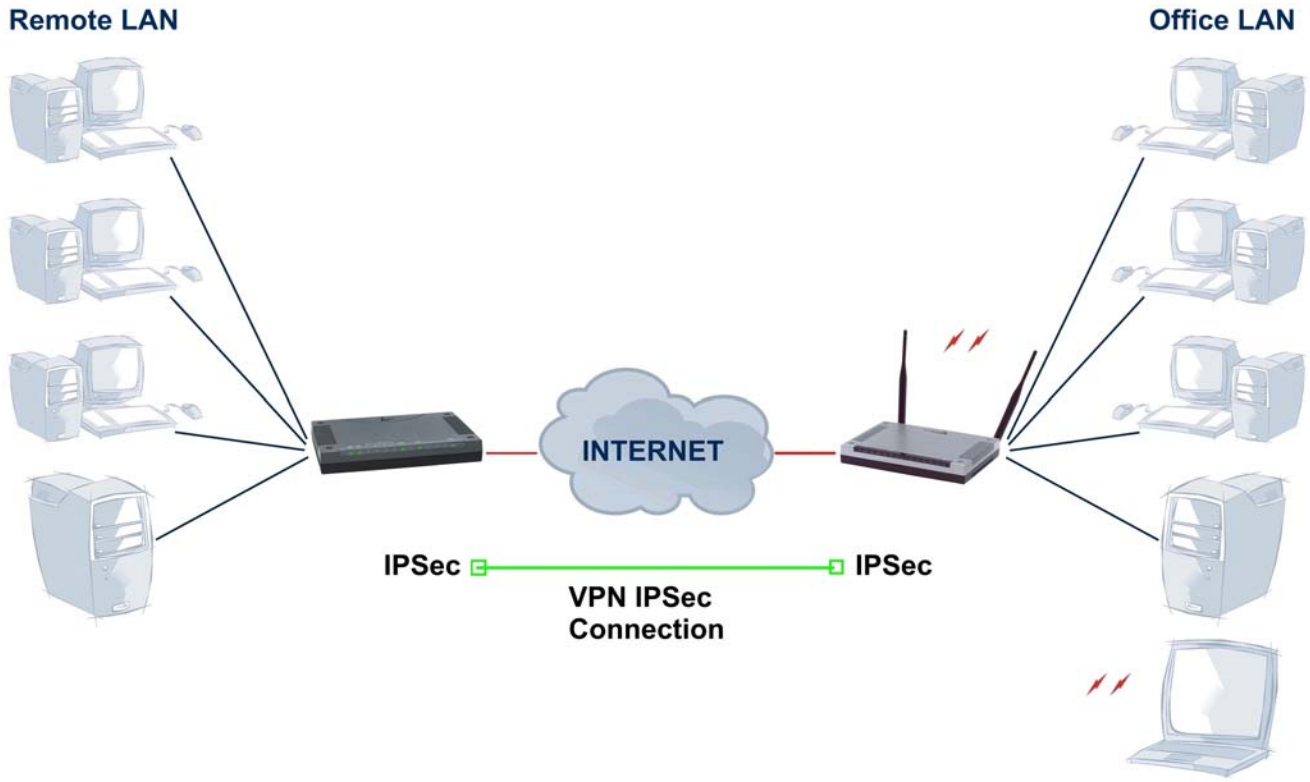
Click **Advanced Option** to change the following settings:



SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. There are two kinds of SAs, IKE and IPSec. IKE negotiates and establishes SA on behalf of IPSec, an IKE SA is used by IKE.
Phase 1 (IKE): To issue an initial connection request for a new VPN tunnel. The range can be from 5 to 15,000 minutes, and the default is 240 minutes.
Phase 2 (IPSec): To negotiate and establish secure authentication. The range can be from 5 to 15,000 minutes, and the default is 60 minutes.
A short SA time increases security by forcing the two parties to update the keys. However, every time the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

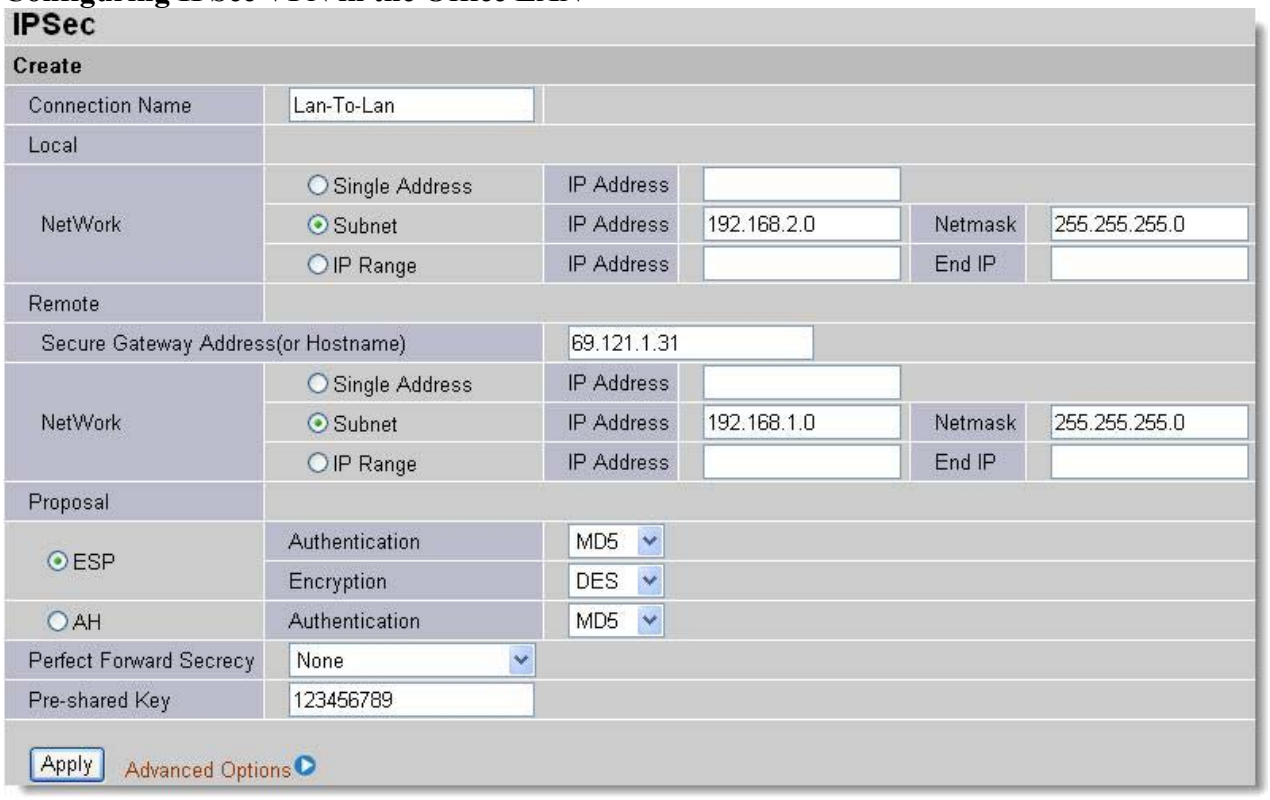
Select the **Apply** button to update the settings.

An Example of Configuring a LAN-to-LAN IPSec VPN Connection

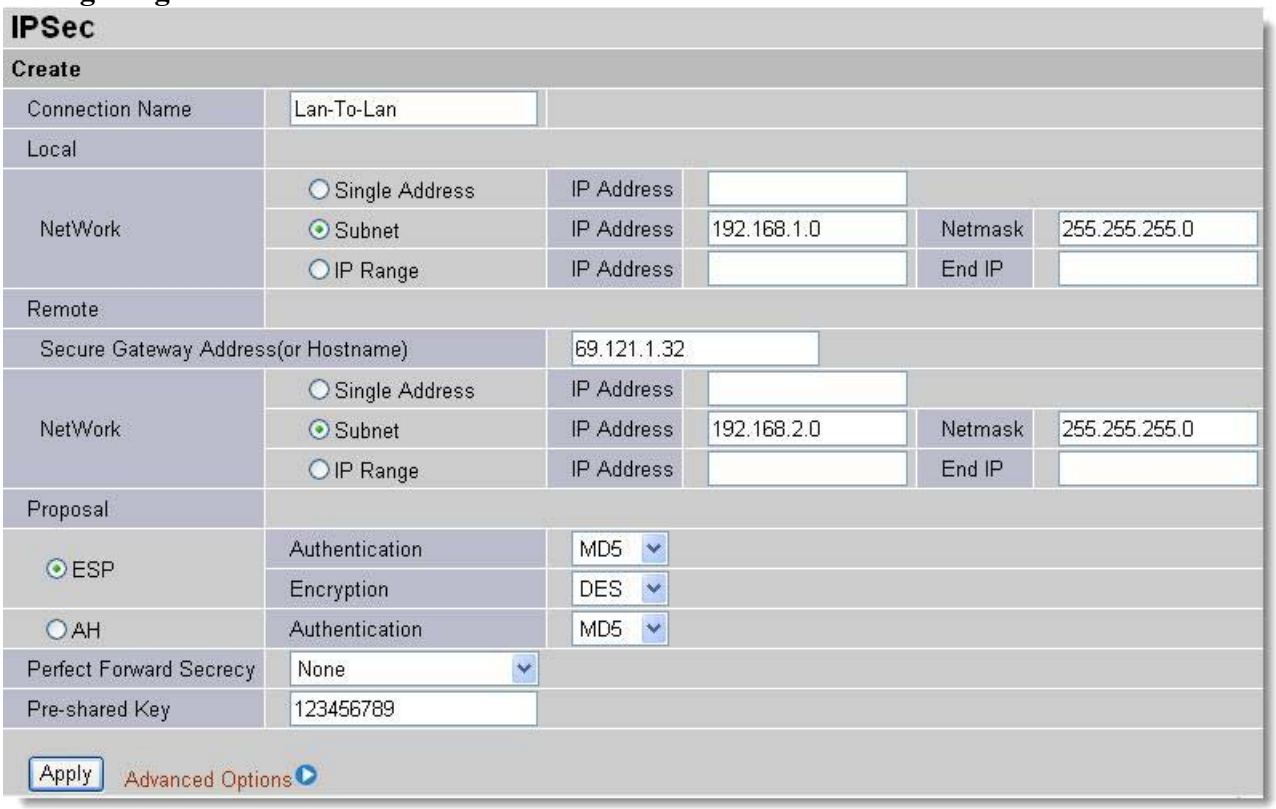


	Remote LAN	Office LAN
Product Code	A02-RA3+	A02-WRA4-54G
Picture		
Public IP	69.121.1.31	69.121.1.32
NAT	Yes	Yes
LAN IP	192.168.1.X	192.168.2.X
Subnet Mask	255.255.255.0	255.255.255.0
VPN IPSec	ESP	ESP
Encryption	DES(or 3DES/AES)	DES(or 3DES/AES)
Authentication	MD5 (or SHA1)	MD5 (or SHA1)
Perfect Forward Secrety	None	None
IKE Pre Shared Key	123456789	123456789

Configuring IPSec VPN in the Office LAN



Configuring IPSec VPN in the Remote LAN



3.6.3.6 QoS

QoS function helps you to control your network traffic for each application from LAN (Ethernet and/or Wireless) to WAN (Internet). It facilitates you to control the different quality and speed of through put for each application when the system is running with full loading of upstream.
You can find two items under the **QoS** section: **Prioritization** and **IP Throttling** (bandwidth management).

3.6.3.6.1 Prioritization

There are three priority settings to be provided in the modem:

- **High**
- **Normal** (The default is normal priority for all of traffic without setting).
- **Low**

The trigger of check can base on IP protocol, port number and address.
And the balance of utilization of each priorities are High(60%), Normal(30%) and Low(10%).

Prioritization

Configuration (from LAN to WAN packet)

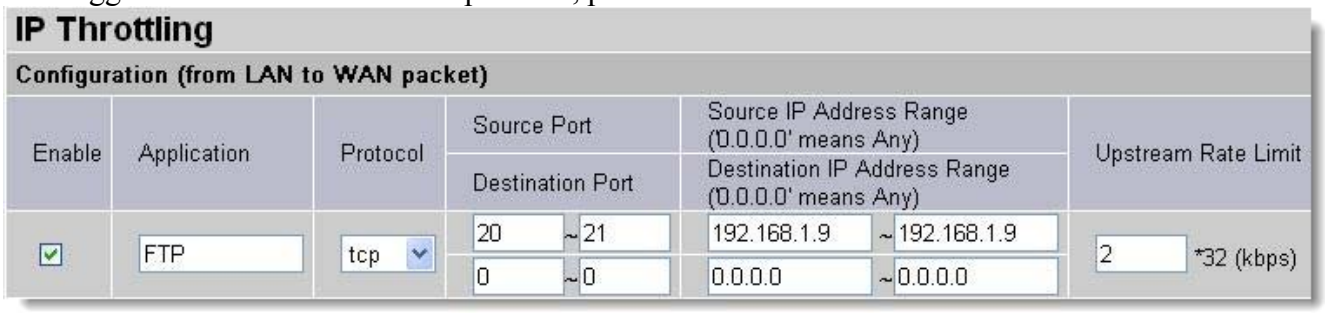
Enable	Application	Priority	Protocol	Source Port / Destination Port	Source IP Address Range ('0.0.0.0' means Any) / Destination IP Address Range ('0.0.0.0' means Any)
☐	PPTP	High	GRE	none / none	~ / ~
☐		High	any	0 ~ 0 / 0 ~ 0	~ / ~
☐		High	any	0 ~ 0 / 0 ~ 0	~ / ~

Enable: Select it to activate the function.
Application: A name that identifies an existing rule.
Priority: High or Low, the priority for existing rule. All of traffic will be set to normal priority until you change it. The balance of utilizations for each priority is High (60%), Normal (30%) or Low (10%).
Protocol: The name of supported protocol.
Source Port: The source port of packets to be monitored.
Destination Port: The destination port of packets to be monitored.
Source IP Address Range: The source IP address or IP range of packets to be monitored.
Destination IP address Range: The destination IP address or IP range of packets to be monitored.

☑	HTTP	High	tcp	0 ~ 0 / 80 ~ 80	192.168.1.5 ~ 192.168.1.5 / 0.0.0.0 ~ 0.0.0.0
☑	SMTP	High	tcp	0 ~ 0 / 25 ~ 25	192.168.1.5 ~ 192.168.1.9 / 0.0.0.0 ~ 0.0.0.0
☑	POP3	High	tcp	0 ~ 0 / 110 ~ 110	192.168.1.10 ~ 192.168.1.20 / 0.0.0.0 ~ 0.0.0.0

3.6.3.6.2 IP Throttling

IP Throttling allows you to limit the speed of IP traffic. The value entered will limit the speed of the application that you set to the specified value's multiple of 32kbps.
The trigger of check can base on IP protocol, port number and address as well.



Enable: Select it to activate the function.
Application: A name that identifies an existing rule.
Protocol: The name of supported protocol.
Source Port: The source port of packets to be monitored.
Destination Port: The destination port of packets to be monitored.
Source IP Address Range: The source IP address or IP range of packets to be monitored.
Destination IP address Range: The destination IP address or IP range of packets to be monitored.
Upstream Rate Limit: This function allows you to limit the speed of IP traffic from LAN to WAN. The value entered will limit the speed of the application that you identified. The speed can be specified in multiple of 32kbps.

3.6.3.7 Virtual Server

When you click Virtual Server, you get the following figure.

Virtual Server

Port Mapping Table — IP Table

Enable	Application	Protocol	External Port	Redirect Port	IP Address
☐	FTP	TCP	21	0 ~ 0	192.168.1.
☐	Telnet	TCP	23	0 ~ 0	192.168.1.
☐	SMTP	TCP	25	0 ~ 0	192.168.1.
☐	HTTP	TCP	80	0 ~ 0	192.168.1.
☐	POP3	TCP	110	0 ~ 0	192.168.1.
☐	NNTP	TCP	119	0 ~ 0	192.168.1.
☐	NTP	UDP	123	0 ~ 0	192.168.1.
☐	HTTPS	TCP	443	0 ~ 0	192.168.1.
☐	IKE	UDP	500	0 ~ 0	192.168.1.
☐	T.120	TCP	1503	0 ~ 0	192.168.1.
☐	H.323	TCP	1720	0 ~ 0	192.168.1.
☐	PPTP	TCP	1723	0 ~ 0	192.168.1.
☐	SIP	TCP/UDP	5060	0 ~ 0	192.168.1.
☐	CUSeeMe	TCP	7648	0 ~ 0	192.168.1.
☐		tcp	0 ~ 0	0 ~ 0	192.168.1.
☐		tcp	0 ~ 0	0 ~ 0	192.168.1.
☐		tcp	0 ~ 0	0 ~ 0	192.168.1.

Being a natural Internet firewall, this network router protects your network from being accessed by outside users. When it needs to allow outside users to access internal servers, e.g. Web server, FTP server, E-mail server or News server, this modem can act as a virtual server. You can set up a local server with specific a port number that stands for the service, e.g. Web (80), FTP (21), Telnet (23), SMTP (25), POP3 (110), When an incoming access request to the router for a specified port is received, it will be forwarded to the corresponding internal server.

For example, if you set the Service Port number 80 (Web) to be mapped to the IP Address 192.168.1.2, then all the http requests from outside users will be forwarded to the local server with IP address of 192.168.1.2. If the port is not listed as a predefined application, you need to add it manually.

DMZ: Regarding the DMZ Host, it is a local computer exposed to the Internet. Therefore, an incoming packet will be checked by the Firewall and NAT algorithms, then passed to the DMZ host when a packet is not sent by a hacker and not limited by the virtual server list.

If you have disabled the NAT option in the WAN-ISP section, this Virtual Server function will hence be invalid.

If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easy way is that the IP address assigned to each virtual server should not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual

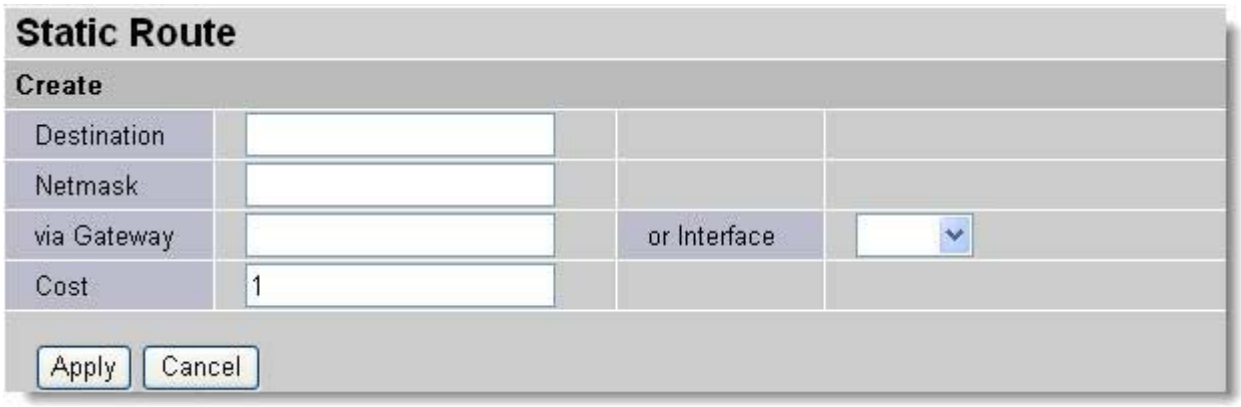
server IP address manually, but it is still in the same subnet with the router.

3.6.3.8 Advanced

There are two items under the Advanced section, Static Routing, Dynamic DNS & Checking Emails.

3.6.3.8.1 Static Routing

Click on the **Static Routing** and then choose **Create IP V4Route** to get the below figure to add a routing table.



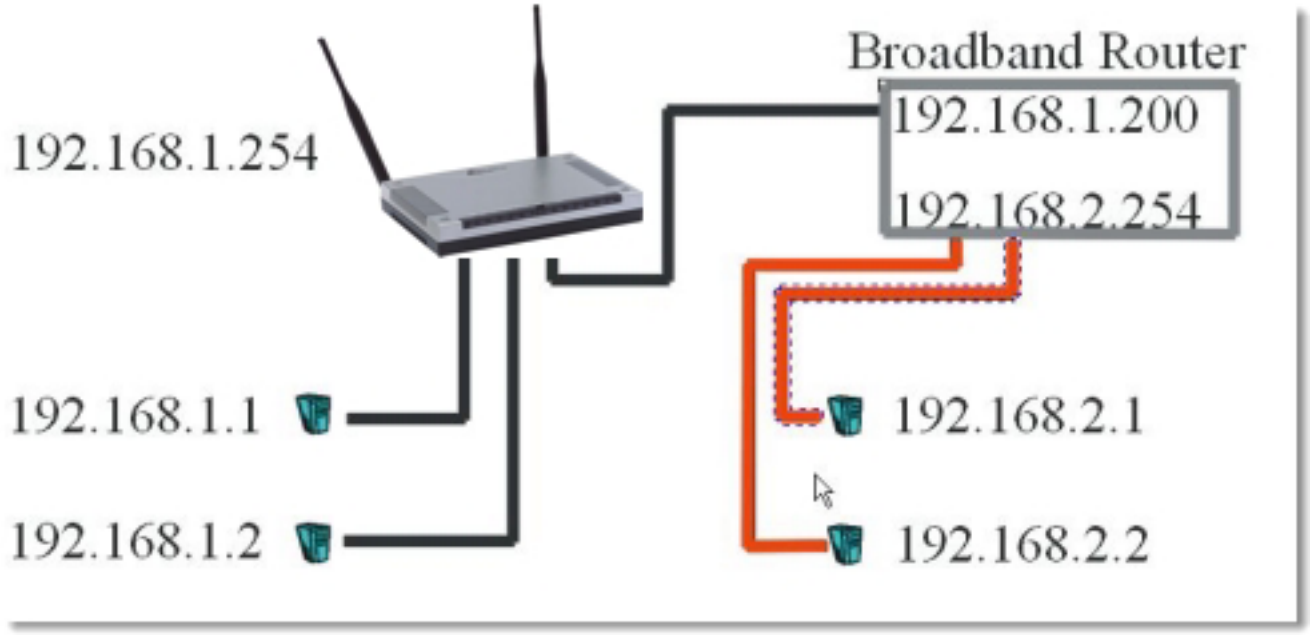
Destination: Enter the destination subnet IP.

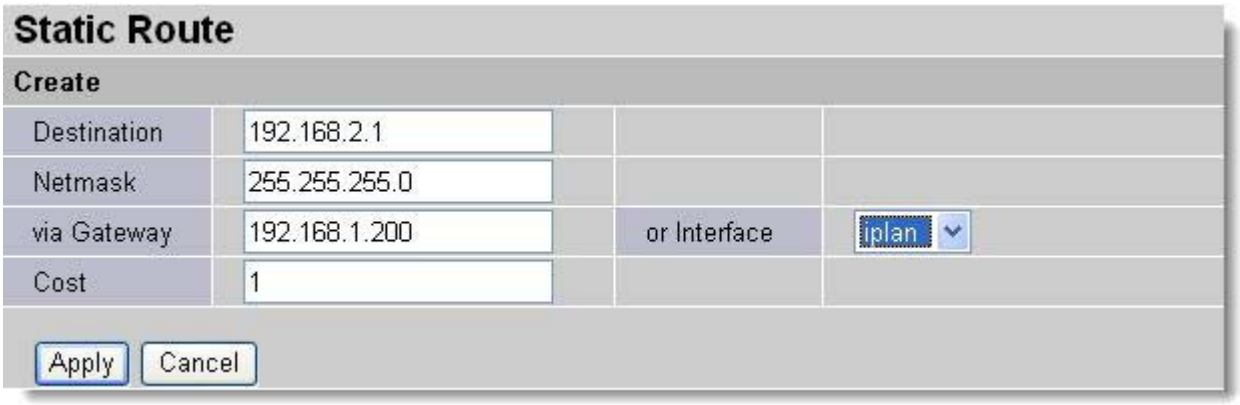
Gateway: Enter the gateway IP address which the packet is forwarded to.

Netmask: Subnet mask of destination IP addresses based on above destination subnet IP.

Cost: This is the same meaning as Hop. Usually, leave it as 1.

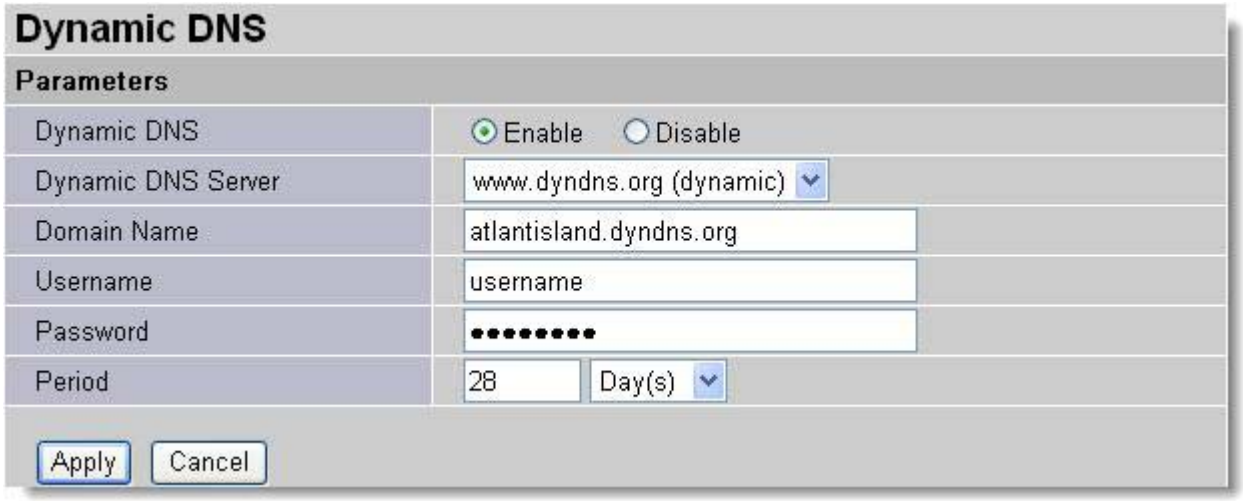
Interface: Enter the interface, which the packet is forwarded to.





3.6.3.8.2 Dynamic DNS

Click **Dynamic DNS** to get the below figure then check the "Enable" button to access the Dynamic DNS service.

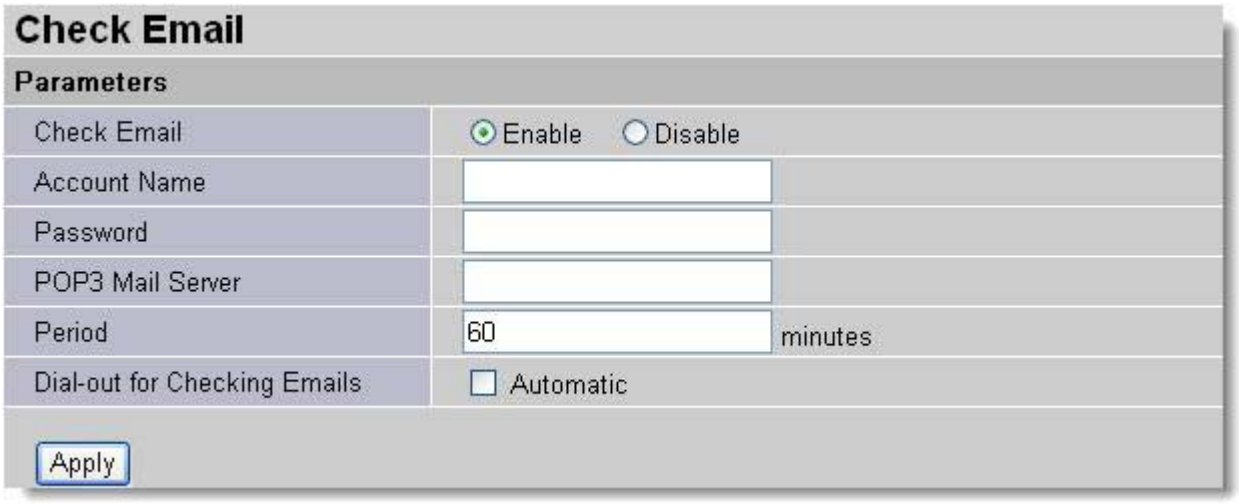


The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. For example, to use the service, you must first apply for an account from this free Web server http://www.dyndns.org/. There are more than 8 DDNS servers supported.

- **Dynamic DNS:** Select the registered DDNS server.
- **Domain Name, Username and Password:** Enter the registered domain name, username and password.
- **Period:** Set the time period for the Router to exchange information with the DDNS server. In addition to update periodically according to this period setting, the Router will take the same action automatically whenever the assigned IP changes.

3.6.3.8.3 Check EMails

Click **Checking Email** to get the below figure then check the "Enable" button to access the service.



⊙ **Disable:** Check to disable the ADSL Firewall Router from getting the email.

⊙ **Enable:** Check to enable the ADSL Firewall Router to get the email by providing required information. Hence, the following fields will be activated and required.

Account Name: Enter the name of the account to which you have the POP access. Normally, it is the text in your email address before the "@" symbol. If you trouble with it, please contact with your ISP.

Password: Enter the password of the account

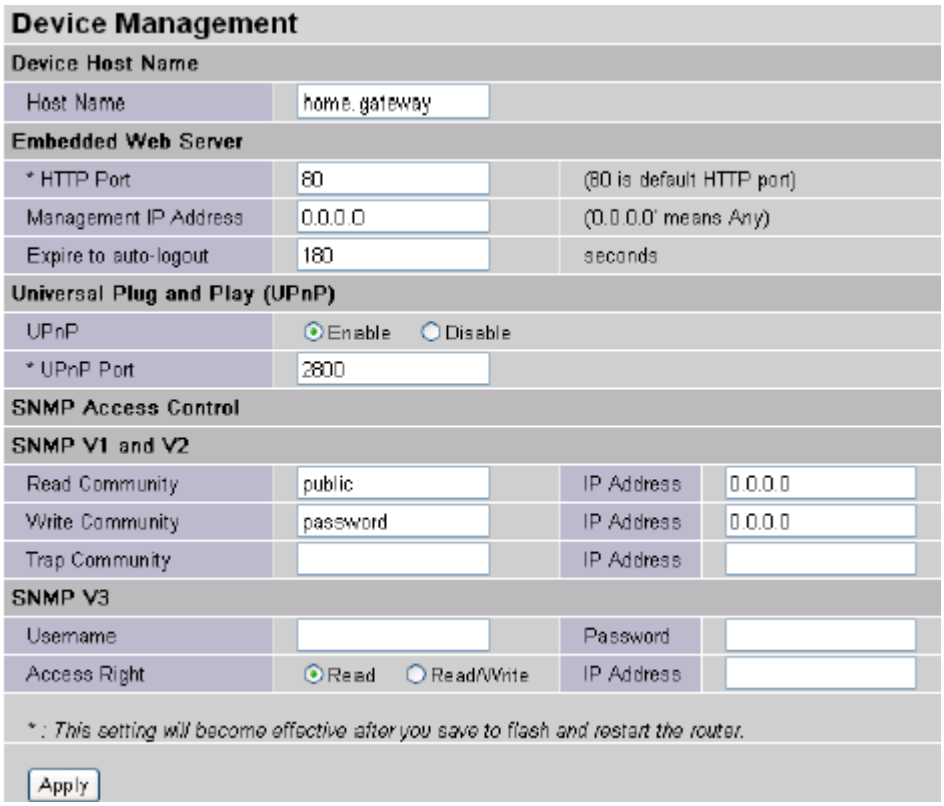
POP3 Mail Server: Enter your (POP) mail server name. If you have trouble with it, you would want to contact your ISP or your external mail server's administrator. For further assistance in tracking down this information, you will need to contact your Internet Service Provider or Network Administrator.

Interval: Enter the value in minute to check your email account periodically.

Automatically dial-out for checking emails: When the function is enabled, your ADSL Firewall Router router will connect to your ISP automatically to check emails if there is your Internet connection dropped. Please be careful when using this feature if your ADSL service is charged by time.

3.6.8.3.4 Device Management

Device Management: Is possible to move the door used for remote configuration of the router, is also possible to block access for a determined period of time and to a precise IP address (leaving instead 0,0,0,0 it is possible to configurare the Router from whichever IP). Is moreover possible Enable/Disable the function Universal Plug and Play and establish the door used for this service. Finally is possible to configure protocol SNMP.



Embedded Web Server:

HTTP Port: This is the port number the router's embedded web server (for web-based configuration) will use. The default value is the standard HTTP port, 80. Users may specify an alternative if, for example, they are running a web server on a PC within their LAN.

Management IP Address: You may specify an IP address allowed to logon and access the router's web server. Setting the IP address to 0.0.0.0 will disable IP address restrictions, allowing users to login from any IP address.

Expire to auto-logout: Specify a time frame for the system to auto-logout the user's configuration session.

For Example: User A changes HTTP port number to 8081, specifies their own IP address of 192.168.1.55, and sets the logout time to be 100 seconds. The router will only allow User A access from the IP address 192.168.1.55 to logon to the Web GUI by typing: http://192.168.1.254:8081 in their web browser. After 100 seconds, the device will automatically logout User A.

Universal Plug and Play (UPnP):

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

- Disable: Check to disable the router's UPnP functionality.
- Enable: Check to enable the router's UPnP functionality.

UPnP Port: Its default setting is 2800. It is highly recommended for users to use this port value. If this value conflicts with other ports already being used you may wish to change the port.

Simple Network Management Protocol:
SNMP Access Control (Software on a PC within the LAN is required in order to utilize this function)
SNMP V1 and V2:

- Read Community: Specify a name to be identified as the Read Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user obtains this IP address will be able to view the data.
- Write Community: Specify a name to be identified as the Write Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be able to view and modify the data.
- Trap Community: Specify a name to be identified as the Trap Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be sent SNMP Traps.

SNMP V3:
Specify a name and password for authentication. And define the access right from identified IP address. Once the authentication has succeeded, users from this IP address will be able to view and modify the data.

SNMP Version: SNMPv2c and SNMPv3
SNMPv2c is the combination of the enhanced protocol features of SNMPv2 without the SNMPv2 security. The "c" comes from the fact that SNMPv2c uses the SNMPv1 community string paradigm for "security", but is widely accepted as the SNMPv2 standard.
SNMPv3 is a strong authentication mechanism, authorization with fine granularity for remote monitoring.

Traps supported: Cold Start, Authentication Failure.
The following MIBs are supported:

- **RFC 1213 (MIB-II):**
  System group
  Interfaces group
  Address Translation group
  IP group
  ICMP group
  TCP group
  UDP group
  EGP (not applicable)
  Transmission
  SNMP group
- **RFC1650 (EtherLike-MIB):**
  dot3Stats
- **RFC 1493 (Bridge MIB):**
  dot1dBase group
  dot1dTp group
  dot1dStp group (if configured as spanning tree)
- **RFC 1471 (PPP/LCP MIB):**
  pppLink group
  pppLqr group
- **RFC 1472 (PPP/Security MIB):**
  PPP Security Group)
- **RFC 1473 (PPP/IP MIB):**

PPP IP Group

- **RFC 1474 (PPP/Bridge MIB):**
  PPP Bridge Group
- **RFC1573 (IfMIB):**
  ifMIBObjects Group
- **RFC1695 (atmMIB):**
  atmMIBObjects
- **RFC 1907 (SNMPv2):**
  only snmpSetSerialNo OID

3.6.4 Save Configuration to Flash

After configuring this network router, you have to save all of the configuration parameters to FLASH.

3.6.5 Logout

To exit the website, choose Logout to exit completely. Please ensure that you have save the configuration settings before logout.

Chapter 4
Troubleshooting

If the ADSL Router is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider. This could save you time and effort but if the symptoms persist, then consult your service provider.

Problems Starting Up the ADSL Firewall Router

Problem	Corrective Action
None of the LEDs are on when you turn on the ADSL Firewall Router.	Check the connection between the adapter and the ADSL Firewall Router. If the error persists, you may have a hardware problem. In this case you should contact technical support.

Problems with the WAN Interface

Problem	Corrective Action
Initialization of the PVC connection failed.	Ensure that the cable is connected properly from the ADSL port to the wall jack. The ADSL LED on the front panel of the ADSL Firewall Router should be on. Check with your VPI, VCI, type of encapsulation and type of multiplexing settings are the same as what you collected from your telephone company and ISP. Reboot the ADSL Firewall Router. If you still have problems, you may need to verify these variables with the telephone company and/or ISP.

Problems with the LAN Interface

Problem	Corrective Action
Can't ping any station on the LAN.	Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a station connected. If it is off, check the cables between your ADSL Firewall Router and the station. Make sure you have uninstalled any software firewall.
	Verify that the IP address and the subnet mask are consistent between the ADSL Firewall Router and the workstations.

APPENDIX A
Specification

Technical Features	
Protocols	IP, NAT, PPTP, ARP, ICMP, DHCP(server, relay and client), PPTP client, RIP1/2 , SNMP, SNTP client, UPnP, Telnet server
LAN port	RJ-45, 4 10/100Base-T ports
WAN port	RJ-11 (1 port ADSL/ADSL2)
Console port	RS232 DB9(9600,8,N,1,N)
External buttons	Reset, Power On/Off
LED Indicators	Power, System, Lan (4), WLAN, MAIL, PPP ed ADSL
Standard ADSL Compliance	ANSI T1.413 Issue 2, ITU-T G.992.1(Full Rate DMT), ITU-T G.992.2 (Lite DMT), ITU-T G.994.1 (Multimode)
Standard ADSL2 Compliance	ITU G.992.3 (G.dmt.bis) (12Mbps download, 1Mbps upload)*
Protocols ADSL	RFC2364(PPPoA), RFC2516(PPPoE), RFC1577 e RFC1483
ATM	ATM AAL2/AAL5 and ATM service class : CBR, UBR, VBR-rt, VBR, ATM Forum UNI 3.0, 3.1 and 4.0
Wireless	Standard IEEE802.11g and IEEE802.11b / Wi-Fi Protected Access (WPA) and WEP 64/128/ Intersil's Nitro Technology [higher overall performance in the real world environment]
Firewall	Intrusion Detection, DoS, Port Filters, URL blocking, MAC blocking
QoS	Quality of Service and IP Throttling
VPN	Accelerator DES/3DES, up to 16 VPN IPSec
Input Power	12V DC @ 1A
Power Consumption	< 10watts
Agency and Regulatory	CE
Dimensions	210 x 145 x 32 mm
Antenna	2*5dBi, external and removable Antenna (reverse SMA)
Weight	<350g
Operating Temperature	0℃ to 40℃
Storage Temperature	-10℃ to 70℃
Operating Humidity	5-95% non-condensing

APPENDIX B
Support

Support

If you have any problems with the I-Fly Wireless ADSL Router, please consult this manual. If you continue to have problems you should contact the dealer where you bought this ADSL Router. If you have any other questions you can contact the Atlantis Land company directly at the following address:

Atlantis Land SpA
Viale De Gasperi, 122
20017 Mazzo di Rho(MI)
Tel: +39. 02.93906085, +39. 02.93907634(help desk)
Fax: +39. 02.93906161

Email: info@atlantis-land.com or tecnici@atlantis-land.com
WWW: http://www.atlantis-land.com

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.